Graduate Algebra Notes

Sean Sather-Wagstaff

Department of Mathematics, 300 Minard Hall, North Dakota State University, Fargo, North Dakota 58105-5075, USA
E-mail address: Sean.Sather-Wagstaff@ndsu.edu
URL: http://math.ndsu.nodak.edu/faculty/ssatherw/

April 29, 2008.

Contents

CHAPTER 1

Group Theory

1. Day 1

DEFINITION 1.1. The *Cartesian product* of two nonempty sets S and T is

$$S \times T = \{(s,t) \mid s \in S, t \in T\}.$$

DEFINITION 1.2. A *binary operation* on a set $S \neq \emptyset$ is a function $\mu\colon S \times S \to S$.

DEFINITION 1.3. A *semigroup* is a nonempty set S coupled with an associative binary operation $S \times S \to S$ denoted $(s, s') \mapsto ss'$.

DEFINITION 1.4. A *monoid* is a semigroup M with a two-sided identity element e_M, sometimes denoted e.

EXAMPLE 1.5. $M = \{0, 1, 2, \ldots\}$ under $+$. This is a monoid.

EXAMPLE 1.6. $M = \{0, 1, 2, \ldots, n\}$ where n is fixed, under $\dot{+}$ where $a \dot{+} b := \min\{a + b, n\}$. This is a monoid.

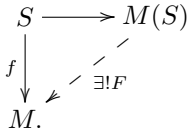
DEFINITION 1.7. Fix a set $S \neq \emptyset$ and set

$$M(S) = \{\text{formal words } s_1 s_2 \cdots s_r \mid s_1, s_2, \ldots, s_r \in S \text{ and } r \geqslant 0\}$$

where the case $r = 0$ produses the "empty word" denoted e. (Formally, $M(S) = (\cup_{r=1}^{\infty} S^r) \cup \{e\} \subseteq S^{(\mathbb{N})} \cup \{e\}$.) Define multiplication on $M(S)$ by concatenation $(s_1 s_2 \cdots s_r)(s'_1 s'_2 \cdots s'_{r'}) := s_1 s_2 \cdots s_r s'_1 s'_2 \cdots s'_{r'}$ and $e(s_1 s_2 \cdots s_r) = s_1 s_2 \cdots s_r = (s_1 s_2 \cdots s_r)e$. (The second part is automatic.) This gives $M(S)$ the structure of a monoid with identity element e, called the *free monoid on* S. We consider S as a subset of $M(S)$ by thinking of S as the set of all words in $M(S)$ with a single character.

DEFINITION 1.8. A *homomorphism of monoids* is a function $f\colon M \to N$ where M and N are monoids such that f preserves multiplication and identities. Abbreviations: hom, hom of monoids, or monoid hom.

PROPOSITION 1.9. *Let S be a nonempty set and M a monoid. Given a function $f\colon S \to M$, there exists a unique monoid homomorphism $F\colon M(S) \to M$ such that $F(s) = f(s)$ for all $s \in S$, that is, such that $F|_S = f$, that is, such that the following diagram commutes:*



PROOF. Define $F(e) = e_M$ and $F(s_1 s_2 \cdots s_r) = f(s_1)f(s_2)\cdots f(s_r)$. Check that this is a well-defined function satisfying the desired properties. □

PROPOSITION 1.10. *The identity element of a monoid is unique.*

PROOF. $e = ee' = e'$. □

DEFINITION 1.11. A *group* is a monoid G such that every element $a \in G$ has a two-sided inverse in G. A group is *abelian* if its operation is commutative.

PROPOSITION 1.12. *Let S be a semigroup. If S admits a left identity and every element of S admits a left inverse, then S is a group.*

PROOF. Let $e \in S$ be a left identity and fix $a \in G$. There exists elements $b, c \in S$ such that $ba = e = cb$. Then

$$b(ab) = (ba)b = eb = b$$

and so

$$ab = e(ab) = (cb)(ab) = ((cb)a)b = (c(ba))b = (ce)b = c(eb) = cb = e.$$

Thus, b is a two-sided inverse for a. Furthermore,

$$ae = a(ba) = (ab)a = ea = a$$

and so e is a two-sided inverse for S. □

The next example shows that we have to be careful about applying the previous result.

EXAMPLE 1.13. Let X be a set and $M = \{\text{functions } f\colon X \to X\}$. Then M is a monoid under composition of functions. An element $f \in M$ has a left inverse if and only if f is injective, and f has a right inverse if and only if f is onto. In particular, there are elements of M which have a left inverse but not a right inverse, and vice versa.

EXERCISE 1.14. Let G be a group and fix $a, b, c \in G$.

(a) If $ab = ac$, then $b = c$.
(b) If $ba = ca$, then $b = c$.
(c) The inverse of a in G is unique. [Assume that b and b' are inverses for a, and show $b = b'$.] [Once this is shown, we write a^{-1} for the unique inverse of a in G.]
(d) $(a^{-1})^{-1} = a$.
(e) $(ab)^{-1} = b^{-1}a^{-1}$.
(f) If $a^2 = a$, then $a = e$.

2. Day 2

EXERCISE 2.1. Let G be a group. If $a^2 = e$ for all $a \in G$, then G is abelian.

REMARK 2.2. Let S be a semgroup. Given elements $a, b, c \in S$, the product abc is unambiguous because of the associative law: $a(bc) = (ab)c$. What about more general products like $abcd$ and so on?

DEFINITION 2.3. Let S be a semigroup and fix elements $a_1, \ldots, a_n \in S$. The *product* $a_1 \ldots a_n = \prod_{i=1}^{n} a_i$ is defined inductively:

$$\prod_{i=1}^{0} a_i = e$$

$$\prod_{i=1}^{1} a_i := a_1$$

$$\prod_{i=1}^{n} a_i := \left(\prod_{i=1}^{n-1} a_i \right) a_n \qquad \text{for } n > 1.$$

REMARK 2.4. Pages 27–28 of Hungerford's text discuss the issue of "meaningful products" and Theorem 1.6 of Hungerford's text shows that the product $a_1 \ldots a_n = \prod_{i=1}^{n} a_i$ can be computed with any order of parentheses. This is called the Generalized Associative Law. Read this part of the text. Also, read 1.8 and 1.9, which discuss exponentiation.

EXERCISE 2.5. (Generalized Commutative Law) Let S be a commutative semigroup and fix elements $a_1, \ldots, a_n \in S$. For any permutation $i_1, \ldots, i_n$ of $1, \ldots, n$ show that $a_{i_1} \ldots a_{i_n} = a_1 \ldots a_n$.

DEFINITION 2.6. A *homomorphism of groups* is a function $f \colon G \to H$ where G and H are groups and $f(gg') = f(g)f(g')$ for all $g, g' \in G$.

REMARK 2.7. Note that we do not require that f preserves identities or inverses. We'll show next that this is automatic.

THEOREM 2.8. *If $f \colon G \to H$ is a homomorphism of groups, then $f(e_G) = e_H$, and $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.*

PROOF. We have $f(e_G)^2 = f(e_G)f(e_G) = f(e_G e_G) = f(e_G)$, and so Exercise 1.14(f) implies $f(e_G) = e_H$. Hence, we have $f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H$ which shows that $f(a^{-1})$ satisfies the defining property of $f(a)^{-1}$, that is, $f(a^{-1}) = f(a)^{-1}$. □

REMARK 2.9. *(False "proof" of $f(e_G) = e_H$.)* We have $f(e_G)f(a) = f(e_G a) = f(a)$, so $f(e_G) = e_H$. This doesn't work because f is not surjective.

Note that this proof can be fixed: $f(e_G)f(a) = f(a)$ implies

$$f(e_G) = f(e_G)f(a)f(a)^{-1} = f(a)f(a)^{-1} = e_H.$$

This is essentially the proof of $a^2 = a \implies a = e$, so this is essentially the same proof as the one above.

PROPOSITION 2.10. *Let M be a monoid and set*

$$G = \{m \in M \mid m \text{ has a two-sided inverse in } M\}.$$

Then G is a group under the operation on M.

PROOF. First, we note that $G \neq \emptyset$ because $e_M \in G$: $e_M^{-1} = e_M$.

Next, observe that G is closed under the operation on M. This is the case because, for all $x, y \in G$ the proof of Exercise 1.14(e) shows that the product xy has a two-sided inverse in M, namely the element $y^{-1}x^{-1}$. Thus, $xy \in G$.

The associativity of the operation on G is inherited from M. The fact that e_M is an identity on G follows from the fact that e_M is the identity on M.

For each $x \in G$, we have $x^{-1} \in M$ and $(x^{-1})^{-1} = x \in M \implies x^{-1} \in G$. $\square$

EXAMPLE 2.11. Let k be a field, e.g., $k = \mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$. The set of $n \times n$ matrices $M = \mathrm{M}_n(k)$ with entries in k is a monoid under matrix multiplication. In the notation of Proposition 2.10, the group G of invertible $n \times n$ matrices is denoted $G = \mathrm{GL}_n(k)$, and is called the *general linear group*.

DEFINITION 2.12. Let S be a semigroup and $T \subset S$ a nonempty subset. For an element $s \in S$, define the *left and right cosets* of s to be

$$sT := \{st \in S \mid t \in T\} \qquad\qquad Ts := \{ts \in S \mid t \in T\}$$

and for $s, s' \in S$, define

$$sTs' := \{sts' \in S \mid t \in T\}.$$

REMARK 2.13. Let S be a semigroup and $T \subset S$ a nonempty subset. For elements $s_1, \ldots, s_m, s'_1, \ldots, s'_n \in S$ the Generalized Associative Law (2.4) shows that the set $s_1 \cdots s_m T a'_1 \cdots s'_n$ is unambiguous.

DEFINITION 2.14. Let G be a group. A *subgroup* of G is a subset $H \subseteq G$ which is itself a group under the operation for G. If H is a subgroup of G, we write $H \leqslant G$. If H is a subgroup of G and $H \neq G$, then H is a *proper subgroup* of G, and we write $H < G$. If $H \leqslant G$ and, for all $h \in H$ and all $g \in G$ we have $ghg^{-1} \in H$, then H is a *normal subgroup* of G, and we write $H \trianglelefteqslant G$. When H is a proper normal subgroup of G, we write $H \triangleleft G$.

EXERCISE 2.15. If $H \leqslant G$, then $e_H = e_G$, and for all $h \in H$ the inverse of h in H is the same as the inverse of h in G.

THEOREM 2.16. *If $H \leqslant G$, then the following conditions are equivalent:*

(i) $H \trianglelefteqslant G$;
(ii) *for all $g \in G$, we have $gHg^{-1} \subseteq H$;*
(iii) *for all $g \in G$, we have $gHg^{-1} = H$;*
(iv) *for all $g \in G$, we have $gH = Hg$;*
(v) *for all $g \in G$, there exist $h, k \in G$ such that $gH = Hh$ and $Hg = kH$.*

PROOF. The implications (i) $\implies$ (ii) and (iii) $\implies$ (iv) $\implies$ (v) are clear.

(ii) $\implies$ (iii). $H = gg^{-1}Hgg^{-1} \subseteq gHg^{-1} \subseteq H$ implies equality at each step.

(v) $\implies$ (i). Set $e = e_G = e_H$. Fix $g \in G$ and $h \in H$. Then there exists $k \in G$ such that $gH = Hk$. Since $e \in H$, we have $g = ge = h_1 k$ for some $h_1 \in H$, and so $k = h_1^{-1} g$. Since $gh = h_2 k$ for some $h_2 \in H$, we have $ghg^{-1} = h_2 k g^{-1} = h_2 h_1^{-1} g g^{-1} = h_2 h_1^{-1} \in H$. $\square$

3. Day 3

EXAMPLE 3.1. If G is abelian, then $H \leqslant G$ if and only if $H \trianglelefteqslant G$.

$\{e\} \trianglelefteqslant G$ and $G \trianglelefteqslant G$.

For each integer n, we have $n\mathbb{Z} \trianglelefteqslant \mathbb{Z}$.

PROPOSITION 3.2. *Let G be a group. A nonempty subset $H \subseteq G$ is a subgroup if and only if $gh^{-1} \in H$ for all $g, h \in H$.*

PROOF. We first show $e_G \in H$. Since $H \neq \emptyset$, there exists $g \in H$, and so our assumption implies $e_G = gg^{-1} \in H$.

It follows easily that e_G is an identity on H under the multiplication from G.

To see that H is closed under inverses, fix $g \in H$. Since $e_G \in H$, our assumption implies $g^{-1} = e_G g^{-1} \in H$.

To see that H is closed under the operation of G, fix $g, h \in H$. Since $h^{-1} \in H$, our assumption implies $gh = g(h^{-1})^{-1} \in H$.

Finally, H inherits associativity from G. □

DEFINITION 3.3. Assume $H \trianglelefteq G$. We obtain an relation $\sim$ on G given by $a \sim b$ if and only if $ab^{-1} \in H$.

EXERCISE 3.4. Assume $H \leqslant G$ and fix $a, b \in G$. Recall that $a \sim b$ if and only if $ab^{-1} \in H$.

(a) The relation $\sim$ is an equivalence relation.
(b) $a \sim b$ if and only if $b \in aH$.
(c) If $H \trianglelefteq G$, then the following conditions are equivalent:
  (i) $a \sim b$;
  (ii) $Ha = Hb$.
  (iii) $aH = bH$;

DEFINITION 3.5. Assume $H \trianglelefteq G$. Let G/H be the set of equivalence classes of G under $\sim$, and let $\overline{g} \in G/H$ denote the equivalence class of g:

$$\overline{g} = \{a \in G \mid a \sim g\}.$$

Equivalently, Exercise 3.4(b) shows that G/H is the collection of cosets of the form gH and $\overline{g} = gH$.

Note the following:
$g \in \overline{g}$.
$\overline{g} = \overline{a}$ if and only if $g \sim a$.
$\overline{g} = \overline{e}$ if and only if $g \in H$.

THEOREM 3.6. *Assume $H \trianglelefteq G$. The assignment $\overline{g}\,\overline{h} := \overline{gh}$ in G/H is well-defined and makes G/H into a group with $e_{G/H} = \overline{e_G}$ and $(\overline{g})^{-1} = \overline{g^{-1}}$.*

PROOF. To show well-definedness of the multiplication, fix $g, h, a, b \in G$ such that $\overline{g} = \overline{a}$ and $\overline{h} = \overline{b}$. We need to show $\overline{gh} = \overline{ab}$. The condition $\overline{g} = \overline{a}$ implies $g \sim a$, and so $ga^{-1} \in H$. Writing $\alpha = ga^{-1} \in H$, we have $g = \alpha a$. Similarly, with $\beta = hb^{-1} \in H$, we have $h = \beta b$. Since $H \trianglelefteq G$ and $\beta \in H$, we have $a\beta a^{-1} \in H$, and so

$$gh(ab)^{-1} = ghb^{-1}a^{-1} = \alpha a \beta b b^{-1} a^{-1} = \underbrace{\alpha}_{\in H}\underbrace{a\beta a^{-1}}_{\in H} \in H.$$

It follows that $gh \sim ab$ and so $\overline{gh} = \overline{g'h'}$.

Associativity is inherited from G:

$$\overline{g}(\overline{hk}) = \overline{g}\overline{hk} = \overline{g(hk)} = \overline{(gh)k} = \overline{ghk} = (\overline{gh})\overline{k}.$$

The identity in G/H is $\overline{e_G}$:

$$\overline{g}\ \overline{e_G} = \overline{ge_G} = \overline{g} \qquad \overline{e_G}\ \overline{g} = \overline{e_G g} = \overline{g}.$$

And we have $(\overline{g})^{-1} = \overline{g^{-1}}$:

$$\overline{g}\,\overline{g^{-1}} = \overline{gg^{-1}} = \overline{e_G} = e_{G/H} \qquad \overline{g^{-1}}\,\overline{g} = \overline{g^{-1}g} = \overline{e_G} = e_{G/H}.$$

□

DEFINITION 3.7. Let $f\colon G \to H$ be a group homomorphism. The *kernel* of f is $\operatorname{Ker}(f) = f^{-1}(e_H)$. The homomorphism f is a *monomorphism* if it is injective. The homomorphism f is an *epimorphism* if it is surjective. The homomorphism f is an *isomorphism* if it is bijective. If there is an isomorphism $g\colon G \to H$, then we say that G and H are *isomorphic* and write $G \cong H$.

EXERCISE 3.8. [First Isomorphism Theorem] Let $f\colon G \to H$ be a group homomorphism.

(a) $\operatorname{Ker}(f) \trianglelefteqslant G$ and $\operatorname{Im}(f) \leqslant H$.
(b) The function $\overline{f}\colon G/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ given by $\overline{g} \mapsto f(g)$ is a well-defined group isomorphism and so $\operatorname{Im}(f) \cong G/\operatorname{Ker}(f)$.
(c) f is a monomorphism if and only if $\operatorname{Ker}(f) = \{e_G\}$.

EXERCISE 3.9. Let G be a group, and let $\{H_\lambda \mid \lambda \in \Lambda\}$ be a collection of subgroups of G.

(a) $\cap_\lambda H_\lambda \leqslant G$.
(b) If $H_\lambda \trianglelefteqslant G$ for all $\lambda \in \Lambda\}$, then $\cap_\lambda H_\lambda \trianglelefteqslant G$.
(c) Give an example of a group G with subgroups H and K such that $H \cup K$ is not a subgroup of G.

DEFINITION 3.10. Let G be a group and $X \subseteq G$ a subset. The *subgroup of G generated by X*, denoted $\langle X\rangle$, is the intersection of all subgroups $H \leqslant G$ such that $X \subseteq H$. If $X = \{x_1, \ldots\}$, we write $\langle X\rangle = \langle x_1, \ldots\rangle$. The group G is *cyclic* if there exists $g \in G$ such that $G = \langle g\rangle$.

EXAMPLE 3.11. If G is a group, then $\langle\emptyset\rangle = \{e\}$ and $\langle G\rangle = G$.

4. Day 4

EXAMPLE 4.1. Let $H \trianglelefteqslant G$.

(a) The function $\pi\colon G \to G/H$ given by $g \mapsto \overline{g}$ is a well-defined epimorphism of groups with $\operatorname{Ker}(\pi) = H$. (E.g., $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.)
(b) π is an isomorphism if and only if $H = \{e_G\}$.
(c) An example of a group G and a normal subgroup $\{e_G\} \neq H \trianglelefteqslant G$ such that $G/H \cong G$: Let $G = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$ and $H = \{0\} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$.

PROPOSITION 4.2. *Let G be a group and $X \subseteq G$ a subset.*

(a) $X \subseteq \langle X\rangle \leqslant G$.
(b) $\langle X\rangle$ *is the unique smallest subgroup of G containing X.*
(c) $\langle X\rangle = \{\prod_{i=1}^r x_i \mid r \geqslant 0$ *and* $x_i \in X$ *or* $x_i^{-1} \in X$ *for* $i = 1, \ldots, r\}$.

PROOF. (a) This follows from the definition of $\langle X\rangle$ and Exercise 3.9(a).

(b) Let $X \subseteq H \leqslant G$. It suffices to show that $\langle X\rangle \subseteq H$. This is immediate from the definition because H is among the subgroups intersected to obtain $\langle X\rangle$.

(c) Set $H = \{\prod_{i=1}^r x_i \mid r \geqslant 0$ and $x_i \in X$ or $x_i^{-1} \in X$ for $i = 1, \ldots, r\}$.

To show $\langle X\rangle \subseteq H$, it suffices to show that H is a subgroup of G containing X; then apply part (b). We have $H \neq \emptyset$ because $e = \prod_{i=1}^0 x_i \in H$. Fix elements $\prod_{i=1}^r x_i, \prod_{i=1}^s y_i \in H$ with $x_i \in X$ or $x_i^{-1} \in X$ for $i = 1, \ldots, r$ and $y_i \in X$ or

$y_i^{-1} \in X$ for $i = 1, \dots, s$. We see easily that

$$\left(\prod_{i=1}^{r} x_i\right)\left(\prod_{i=1}^{s} y_i\right)^{-1} = \left(\prod_{i=1}^{r} x_i\right)\left(\prod_{i=1}^{s} y_{s-i}^{-1}\right) \in H.$$

Hence, Proposition 3.2 implies $H \leqslant G$. And $X \subseteq H$ because $x_1 \in X$ implies $x_1 = \prod_{i=1}^{1} x_i \in H$.

Next, we show $\langle X \rangle \supseteq H$. We know $X \subseteq \langle X \rangle$. Since $\langle X \rangle$ is a subgroup, $x_i \in X \subseteq \langle X \rangle$ implies $x_i^{-1} \in \langle X \rangle$. Since $\langle X \rangle$ is closed under products, this implies that elements $\prod_{i=1}^{r} x_i$ are in $\langle X \rangle$. That is, $H \subseteq \langle X \rangle$. □

Exercise 4.3. If $H \leqslant \mathbb{Z}$, then $H = n\mathbb{Z} = \langle n \rangle$ for some $n \geqslant 0$.

Theorem 4.4. *Let G be a group. If $g \in G$, then either $\langle g \rangle \cong \mathbb{Z}$ or $\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$ for some $n \geqslant 1$.*

Proof. Let $f\colon \mathbb{Z} \to \langle g \rangle$ be given by $m \mapsto g^m$. This is a well-defined group epimorphism, so Exercise 3.8(b) implies $\mathbb{Z}/\operatorname{Ker}(f) \cong \operatorname{Im}(f) = \langle g \rangle$.

The condition $\operatorname{Ker}(f) \leqslant \mathbb{Z}$ implies $\operatorname{Ker}(f) = n\mathbb{Z}$ for some $n \geqslant 0$, by Exercise 4.3. If $n = 0$, then $\langle g \rangle \cong \mathbb{Z}/\operatorname{Ker}(f) = \mathbb{Z}/\{0\} \cong \mathbb{Z}$. If $n > 0$, then $\langle g \rangle \cong \mathbb{Z}/\operatorname{Ker}(f) = \mathbb{Z}/n\mathbb{Z}$. □

Definition 4.5. Let G be a group and $H \leqslant G$. The *order* of G is the cardinality $|G|$. The *index* of H in G is

$$[G\colon H] = \text{the number of distinct cosets of } H \text{ in } G.$$

Theorem 4.6 (Lagrange's Theorem). *Let G be a finite group. If $H \leqslant G$, then $|G| = [G\colon H]|H|$; in particular, $|H| \mid |G|$.*

5. Day 5

Proof. We first show, for all $g \in G$, that $|gH| = |H|$. Let $\varphi_g\colon H \to gH$ be given by $h \mapsto gh$. By definition, φ_g is onto, and it is 1-1 because $gh = gh' \implies h = h'$.

Let $G/H = \{gH \mid g \in G\}$. (Note that we're not assuming that H is a normal subgroup, so G/H is just a set.) Since $\sim$ is an equivalence relation, G is the disjoint union of its cosets:

$$G = \bigcup_{gH \in G/H} gH.$$

Thus, we have

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = [G : H]|H|.$$

□

Definition 5.1. Let G be a group, and fix a subset $\emptyset \neq S \subseteq G$. The *normalizer* of S in G is

$$N_S = \{x \in G \mid xSx^{-1} = S\}.$$

If $S = \{x\}$, then we write $N_S = N_x$.

Theorem 5.2. *Let G be a group. If $\emptyset \neq S \subseteq G$, then $N_S \leqslant G$.*

PROOF. We have $e \in S$ since $eSe^{-1} = eSe = S$.
For $x, y \in N_S$, we have $xy \in N_S$ because

$$xyS(xy)^{-1} = xySy^{-1}x^{-1} = xSx^{-1} = S.$$

For $x \in N_S$, we have $x^{-1} \in N_S$ because

$$x^{-1}S(x^{-1})^{-1} = x^{-1}Sx = x^{-1}xSx^{-1}x = S.$$

Now apply Proposition 3.2. □

DEFINITION 5.3. If G is a group with subgroups $H, K \leqslant G$, then

$$HK = \{hk \mid h \in H \text{ and } k \in K\}.$$

EXAMPLE 5.4. If G is a group with subgroups $H, K \leqslant G$, then HK may not be a subgroup of G.

For each integer $n \geqslant 1$, the *symmetric group on n letters* is

$$S_n = \{\text{bijections } f\colon \{1, \dots, n\} \to \{1, \dots, n\}\}.$$

In S_3, set $\sigma = (1\,2)$ and $\delta = (2\,3)$. Check that

$$\begin{aligned} H &:= \langle\sigma\rangle = \{(1), \sigma\} \\ K &:= \langle\delta\rangle = \{(1), \delta\} \\ HK &= \{(1), \sigma, \delta, \sigma\delta\} = \{(1), (1\,2), (2\,3), (1\,2\,3)\} \end{aligned}$$

Then HK is not a group because $\delta, \sigma \in HK$ and $\delta\sigma = (1\,3\,2) \notin HK$.

THEOREM 5.5. *Let G be a group with subgroups $H, K \leqslant G$. If $H \subseteq N_K$, then $HK \leqslant G$.*

PROOF. Since $e \in H$ and $e \in K$, we have $e = ee \in HK$.
For $h_1k_1, h_2k_2 \in HK$, we have

$$h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = \underbrace{h_1h_2^{-1}}_{\in H}\underbrace{h_2k_1k_2^{-1}h_2^{-1}}_{\in K} \in HK.$$

Now apply Proposition 3.2. □

EXAMPLE 5.6. If G is abelian, then $N_S = G$ for all $\emptyset \neq S \subseteq G$, and so $HK \trianglelefteq G$ for all $H, K \leqslant G$.

THEOREM 5.7. *Let G be a finite group with subgroups $H, K \leqslant G$. Then $|HK| = |H||K|/|H \cap K|$.*

PROOF. Define $\mu\colon H \times K \to HK$ by the formula $(h, k) \mapsto hk$. This map is onto by definition.

Claim: $\mu(h_1, k_1) = \mu(h_2, k_2)$ if and only if $h_2 = h_1a^{-1}$ and $k_2 = ak_1$ for some $a \in H \cap K$.

($\Longleftarrow$) If such an $a \in H \cap K$ exists, then

$$\mu(h_2, k_2) = \mu(h_1a^{-1}, ak_1) = h_1a^{-1}ak_1 = h_1k_1 = \mu(h_1, k_1).$$

($\Longrightarrow$) If $\mu(h_1, k_1) = \mu(h_2, k_2)$, then $h_1k_1 = h_2k_2$ and so $\underbrace{h_2^{-1}h_1}_{\in H} = \underbrace{k_2k_1^{-1}}_{\in K}$. Set $a = h_2^{-1}h_1 = k_2k_1^{-1}$ which is in $H \cap K$, and check that $h_2 = h_1a^{-1}$ and $k_2 = ak_1$.

For all $h \in H$ and $k \in K$, set

$$L_{h,k} = \{(ha^{-1}, ak) \mid a \in H \cap K\}.$$

The claim implies

$$|HK| = \text{the number of distinct } L_{h,k}.$$

Also, $H \times K$ is the disjoint union of the $L_{h,k}$. Also,

$$|L_{h,k}| = |H \cap K|.$$

Hence,

$$|H||K| = |H \times K| = \sum_{\substack{\text{distinct} \\ L_{h,k}}} |L_{h,k}| = \sum_{\substack{\text{distinct} \\ L_{h,k}}} |H \cap K| = |HK||H \cap K|.$$

□

6. Days 6 and 7

EXAMPLE 6.1. Let G and H be groups. The Cartesian product $G \times H$ is a group under the "coordinatewise" operation

$$(g, h)(g', h') = (gg', hh')$$

with $e_{G\times H} = (e_G, e_H)$ and $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Let $i_G \colon G \to G \times H$ be given as $i_G(g) = (g, e_H)$. Then i_G is a group monomorphism. Furthermore, $\operatorname{Im}(i_G) \trianglelefteq G \times H$ and $(G \times H)/\operatorname{Im}(i_G) \cong H$.

Let $i_H \colon H \to G \times H$ be given as $i_H(h) = (e_G, h)$. Then i_H is a group monomorphism. Furthermore, $\operatorname{Im}(i_H) \trianglelefteq G \times H$ and $(G \times H)/\operatorname{Im}(i_H) \cong G$.

(We often identify G and H with their images in $G \times H$, in which case the isomorphisms read $(G \times H)/G \cong H$ and $(G \times H)/H \cong G$.

EXAMPLE 6.2. Let G and H be groups.

Let $\mathrm{id}_G \colon G \to G$ be given by $\mathrm{id}_G(g) = g$. This is the *identity isomorphism* on G; it is a group isomorphism.

Let $f \colon G \to H$ be given by $f(g) = e_H$ for all $g \in G$; it is a group homorphism.

DEFINITION 6.3. Let G be a group, and fix a subset $\emptyset \neq S \subseteq G$. The *centralizer* of S in G is

$$Z_S = \{g \in G \mid gs = sg \text{ for all } s \in S\}.$$

The *center* of G is

$$Z(G) = Z_G = \{g \in G \mid gg' = g'g \text{ for all } g' \in G\}.$$

THEOREM 6.4. *Let G be a group, and fix a subset $\emptyset \neq S \subseteq G$. Then $Z_S \leqslant G$ and $Z(G) \trianglelefteq G$.*

PROOF. $e \in Z_S$ because $es = s = se$.

For $x, y \in Z_S$ we have $xy \in Z_S$ because $xys = xsy = sxy$.

For $x \in Z_S$, we have $x^{-1} \in Z_S$ because

$$x^{-1}sx = x^{-1}xs = s = sx^{-1}x$$

and so cancellation implies $x^{-1}x = sx^{-1}$.

It follows that $Z(G) = Z_G \leqslant G$, so we need to check normalcy: for $x \in Z(G)$ and $g \in G$, we have $xg = gx$ and so $gxg^{-1} = xgg^{-1} = x \in Z(G)$. □

EXAMPLE 6.5. Let G be a group, and fix a subset $\emptyset \neq S \subseteq G$. Then $Z_S \leqslant N_S$.

THEOREM 6.6 (Second Isomorphism Theorem). *Let $H, K \trianglelefteq G$ with $K \subseteq H$.*

(a) $K \trianglelefteq H$
(b) $H/K \trianglelefteq G/K$
(c) *The function* $\tau\colon G/K \to G/H$ *given by* $\tau(gH) = gK$ *is a well defined group epimorphism with* $\operatorname{Ker}(\tau) = H/K$. *In particular,* $(G/K)/(H/K) \cong G/H$.

PROOF. (a) easy.

(b) It is straightforward to show that $H \leqslant G$ implies $H/K \leqslant G/K$: H/K is nonempty because H is; it is closed under the operation in G/K because H is closed under the operation in G; and it is closed under inverses in G/K because H is closed under inverses in G.

For $h \in H$ and $g \in G$, we have $ghg^{-1} \in H$ because $H \trianglelefteq G$, and so

$$\overline{g}\overline{h}\overline{g}^{-1} = \overline{g}\overline{h}\overline{g^{-1}} = \overline{ghg^{-1}} \in H/K.$$

(c) Well-definedness. If $gK = aK$, then $ga^{-1} \in K \subseteq H$, and so $gH = aH$.

It is straightforward to check that τ is a group epimorphism. For the kernel: $gK \in \operatorname{Ker}(\tau)$ if and only if $gH = eH = H$ if and only if $g \in H$ if and only if $gK \in H/K$. The final statement follows from the First Isomorphism Theorem 3.8:

$$G/H = \operatorname{Im}(\tau) \cong (G/K)/\operatorname{Ker}(\tau) = (G/K)/(H/K).$$

□

THEOREM 6.7. *Let* $H, K \leqslant G$ *with* $H \subseteq N_K$.

(a) $K \trianglelefteq HK$
(b) $H \cap K \trianglelefteq H$
(c) *The function* $\phi\colon H/(H \cap K) \to (HK)/K$ *given by* $\phi(h(H \cap K)) = hK$ *is a well defined group isomorphism. In particular,* $H/(H \cap K) \cong (HK)/K$.

PROOF. (a) Recall that $HK \leqslant G$ because $H \subseteq N_K$ by Theorem 5.5. Since $e \in H$, we have $K = eK \subseteq HK$. It follows easily that $K \leqslant HK$. For normalcy, fix $hk \in HK$ and $k' \in K$. Then

$$hkk'(hk)^{-1} = h\underbrace{kk'k^{-1}}_{\in K}h^{-1} \subseteq hKh^{-1} = K$$

where the last equality comes from $h \in H \subseteq N_K$.

(b) and (c) As above, we have $H \leqslant HK \leqslant G$. Let $\pi\colon H \to (HK)/K$ be given by $\pi(h) = hK$. One checks readily that π is a well-defined group homomoprhism.

We claim that π is surjective with $\operatorname{Ker}(\pi) = H \cap K$. Once this is done, we will have $H \cap K \trianglelefteq H$ by Exercise 3.8(a). Furthermore, Exercise 3.8(b) then implies that the function $\tau\colon H/(H \cap K) \to (HK)/K$ given by $\tau(h(H \cap K)) = \pi(h) = hK$ is a well-defined group isomorphism and so $H/(H \cap K) \cong (HK)/K$.

π is surjective: for each $hk \in HK$, we have

$$hkK = hK = \pi(h).$$

To see $\operatorname{Ker}(\pi) \supseteq H \cap K$, fix $k \in H \cap K$:

$$\pi(k) = kK = K = e_{HK/K}.$$

To see $\operatorname{Ker}(\pi) \subseteq H \cap K$, fix $x \in \operatorname{Ker}(\pi) \subseteq H$. Then $x \in H$ and $\pi(x) = e_{HK/K}$, that is, $xK = K$. Hence, $x \in K$ and so $x \in H \cap K$. □

Day 7

THEOREM 6.8. *Let $H, K \leqslant G$ such that $H \cap K = \{e\}$ and $HK = G$. If $H \subseteq Z_K$ (that is, if $hk = kh$ for all $h \in H$ and all $k \in K$), then the function $f\colon H \times K \to G$ given by $f(h,k) = hk$ is an isomorphism,*

PROOF. The function is well-defined. It is surjective because $G = HK$. It is a homomorphism because

$$f((h,k)(h',k')) = f(hh', kk') = hh'kk' = hkh'k' = f(h,k)f(h',k').$$

The first equality in the next sequence is by definition:

$$\mathrm{Ker}(f) = \{(h,k) \in H \times K \mid hk = e\} = \{(e,e)\} = \{e_{H\times K}\}.$$

For the second equality, the containment $\supseteq$ is easy. For the containment $\subseteq$, if $hk = e$, then $k^{-1} = h \in H \cap K = \{e\}$ implies $h = e$ and $k = h^{-1} = e^{-1} = e$.

Hence, f is injective by Exercise 1 in assignment 2, that is, Exercise 3.8(c). □

EXERCISE 6.9. Let $f\colon G \to G'$ be a group homomorphism.

(a) If $H' \leqslant G'$, then $f^{-1}(H') \leqslant G$.
(b) If $H' \trianglelefteq G'$, then $f^{-1}(H') \trianglelefteq G$.
(c) If $H' \trianglelefteq G'$, then the function $\overline{f}\colon G/f^{-1}(H') \to G'/H'$ is a well-defined group monomorphism

THEOREM 6.10. *Let $K \trianglelefteq G$ and let $\pi\colon G \to G/K$ be the group epimorphism $\pi(g) = gK$.*

(a) *There is a 1-1 correspondence*

$$\{H \leqslant G \mid K \subseteq H\} \longleftrightarrow \{H' \leqslant G/K\}$$

given by

$$H \longmapsto H/K$$
$$\pi^{-1}(H') \longmapsfrom H'$$

(b) *There is a 1-1 correspondence*

$$\{H \trianglelefteq G \mid K \subseteq H\} \longleftrightarrow \{H' \trianglelefteq G/K\}$$

given by

$$H \longmapsto H/K$$
$$\pi^{-1}(H') \longmapsfrom H'$$

PROOF. This follows from the Second Isomorphism Theorem 6.6 (and the ideas in its proof) and Exercise 6.9. □

DEFINITION 6.11. A group $G \neq \{e\}$ is *simple* if its only normal subgroups are G and $\{e\}$. See Example 3.1.

EXERCISE 6.12. If G is a simple abelian group, then $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime number p.

7. Day 8

DEFINITION 7.1. Let G be a group. A *tower* of subgroups of G (or a *normal series* in G) is a chain $\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$. Each group G_k/G_{k+1} is a *factor* of the series. The series is *abelian* if each factor is abelian. The series is *cyclic* if each factor is cyclic. If each nontrivial factor is simple, then the series is called a *composition series*. A normal series $\{e\} = H_m \trianglelefteq H_{m-1} \trianglelefteq \cdots \trianglelefteq H_0 = G$ is a *refinement* of the original series if there is a sequence $k_1 < k_2 < \cdots < k_n$ such that $H_{k_j} = G_j$ for $j = 1, \ldots, n$.

The group G is *solvable* if it has an abelian normal series.

Two normal series in G are *equivalent* if they have the same nontrivial factors up to reordering and isomorphism.

LEMMA 7.2. *Let $H, H', K \leqslant G$. If $H' \trianglelefteq H \subseteq N_K$, then $H'K \trianglelefteq HK$.*

PROOF. Theorem 5.5 implies $H'K \leqslant G$ and $HK \leqslant G$, and so the containment $H'K \subseteq HK$ implies $H'K \leqslant HK$. By Theorem 6.7(a), it suffices to show $H \subseteq N_{H'K}$ because then we will have $H'K \trianglelefteq HH'K = HK$.

Fix $h \in H$. Because $H' \trianglelefteq H$, we have $hH'h^{-1} = H'$. And $H \subseteq N_K$ implies $hKh^{-1} = K$. Hence, we have

$$hH'Kh^{-1} = hH'h^{-1}hKh^{-1} = H'K$$

and so $H'K \trianglelefteq HK$. □

THEOREM 7.3 (Jordan-Hölder Theorem). *If G is a group, then any two normal series have equivalent refinements.*

PROOF. Consider normal series

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G \tag{7.3.1}$$

and

$$\{e\} = H_m \trianglelefteq H_{m-1} \trianglelefteq \cdots \trianglelefteq H_0 = G. \tag{7.3.2}$$

The plan is to augment (7.3.1) by inserting a sequence of the following form at each step:

$$G_{k+1} = (H_m \cap G_k)G_{k+1} \trianglelefteq (H_{m-1} \cap G_k)G_{k+1} \trianglelefteq \cdots \trianglelefteq (H_0 \cap G_k)G_{k+1} = G_k.$$

This will be a refinement of (7.3.1). We will then find a similar refinement of (7.3.2) which and we will show that these refinements are equivalent.

For each $k = 0, \ldots, n-1$, we have a normal series

$$\{e\} = H_m \cap G_k \trianglelefteq H_{m-1} \cap G_k \trianglelefteq \cdots \trianglelefteq H_0 \cap G_k = G_k$$

by Exercise 3.9(b).

The condition $G_{k+1} \trianglelefteq G_k$ implies $H_{i-1} \cap G_k \subseteq G_k \subseteq N_{G_{k+1}}$. Hence, we may apply Lemma 7.2 with $H' = H_i \cap G_k \trianglelefteq H_{i-1} \cap G_k = H$ and $K = G_{k+1}$ in order to conclude

$$(H_i \cap G_k)G_{k+1} \trianglelefteq (H_{i-1} \cap G_k)G_{k+1}.$$

Furthermore, we have

$$G_{k+1} = \{e\}G_{k+1} = (H_m \cap G_k)G_{k+1} \qquad \text{and} \qquad G_k = G_kG_{k+1} = (H_0 \cap G_k)G_{k+1}$$

and so

$$G_{k+1} = (H_m \cap G_k)G_{k+1} \trianglelefteq (H_{m-1} \cap G_k)G_{k+1} \trianglelefteq \cdots \trianglelefteq (H_0 \cap G_k)G_{k+1} = G_k.$$

Putting these sequences together for $k = 0, \dots, n-1$ yields a refinement

$$\{e\} = (H_m \cap G_{n-1})G_n \trianglelefteq \cdots \trianglelefteq (H_1 \cap G_0)G_1 \trianglelefteq (H_0 \cap G_0)G_1 = G_0 = G \tag{7.3.3}$$

of the normal series (7.3.1).

Similarly, the series

$$\{e\} = (H_{m-1} \cap G_n)H_m \trianglelefteq \cdots \trianglelefteq (H_0 \cap G_1)H_1 \trianglelefteq (H_0 \cap G_0)H_1 = H_0 = G \tag{7.3.4}$$

is a refinement of the normal series (7.3.2).

To show that the series (7.3.3) and (7.3.4) are equivalent, it suffices to show

$$\frac{(G_i \cap H_j)G_{i+1}}{(G_i \cap H_{j+1})G_{i+1}} \cong \frac{(H_j \cap G_i)H_{j+1}}{(H_j \cap G_{i+1})H_{j+1}}$$

since this will give the bijection between the factors.

Set $H = G_i \cap H_j$ and $K = (G_i \cap H_{j+1})G_{i+1}$. Then

$$HK = (G_i \cap H_j)(G_i \cap H_{j+1})G_{i+1} = (G_i \cap H_j)G_{i+1}$$

and so Theorem 6.7(c) implies

$$\frac{(G_i \cap H_j)G_{i+1}}{(G_i \cap H_{j+1})G_{i+1}} = \frac{HK}{K} \cong \frac{H}{H \cap K} = \frac{G_i \cap H_j}{(G_i \cap H_{j+1})G_{i+1} \cap G_i \cap H_j}.$$

Similarly, we have

$$\frac{(G_i \cap H_j)H_{j+1}}{(G_{i+1} \cap H_j)H_{j+1}} \cong \frac{G_i \cap H_j}{(G_{i+1} \cap H_j)H_{j+1} \cap G_i \cap H_j}$$

so it suffices to show

$$(G_i \cap H_{j+1})G_{i+1} \cap G_i \cap H_j = (G_{i+1} \cap H_j)H_{j+1} \cap G_i \cap H_j.$$

"$\subseteq$" Fix an element

$$\alpha \in (G_i \cap H_{j+1})G_{i+1} \cap G_i \cap H_j \subseteq (G_i \cap H_{j+1})G_{i+1} = G_{i+1}(G_i \cap H_{j+1}).$$

The last equality holds because $G_i \cap H_{j+1} \subseteq G_i \subseteq N_{G_{i+1}}$. It follows that $\alpha = \beta\gamma$ for some $\beta \in G_{i+1}$ and $\gamma \in G_i \cap H_{j+1}$. Then $\beta = \alpha\gamma^{-1} \in H_j$ because $\alpha \in H_j$ and $\gamma^{-1} \in H_{j+1} \subseteq H_j$. It follows that

$$\alpha = \beta\gamma \in (G_{i+1} \cap H_j)H_{j+1} \cap G_i \cap H_j.$$

This establishes "$\subseteq$", and "$\supseteq$" is verified similarly. □

8. Day 9

COROLLARY 8.1. *If G is a group, then any two composition series in G are equivalent.*

PROOF. By Theorem 7.3 it suffices to show that any composition series

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

is equivalent to any refinement of itself. Suppose that the refinement has one additional subgroup

$$G_{k+1} \trianglelefteq H \trianglelefteq G_k.$$

Since $H/G_{k+1} \trianglelefteq G_k/G_{k+1}$ and G_k/G_{k+1} is simple, we have either $H/G_{k+1} = \{e_{G_k/G_{k+1}}\}$ or $H/G_{k+1} = G_k/G_{k+1}$. That is, we have $H = G_{k+1}$ or $H = G_k$, so no new nontrivial factors were introduced.

The result follows by induction on the number of new subgroups introduced to make the refinement. □

Every group has a normal series: $\{e\} \trianglelefteqslant G$. The next example show that not every group has a composition series.

EXAMPLE 8.2. The subgroups of $\mathbb{Z}$ are all of the form $n\mathbb{Z}$ with $n \geqslant 0$, and $\mathbb{Z}/n\mathbb{Z}$ is simple if and only if n is prime. If $n \geqslant 1$, then $n\mathbb{Z} \cong \mathbb{Z}$. Hence, given a normal series

$$\{0\} = n_m\mathbb{Z} \trianglelefteqslant n_{m-1}\mathbb{Z} \trianglelefteqslant \cdots \trianglelefteqslant n_0\mathbb{Z} = \mathbb{Z}$$

if $n_{m-1} \neq 0$ then

$$n_{m-1}\mathbb{Z}/n_m\mathbb{Z} = n_{m-1}\mathbb{Z}/\{0\} \cong n_{m-1}\mathbb{Z} \cong \mathbb{Z}$$

and this group is not simple. Hence the normal series is not a composition series.

COROLLARY 8.3. *Assume that G is solvable. If G has a composition series $\{e\} = G_n \trianglelefteqslant G_{n-1} \trianglelefteqslant \cdots \trianglelefteqslant G_0 = G$, then there exist prime numbers $p_1, \ldots, p_n$ such that $G_{i-1}/G_i \cong \mathbb{Z}/p\mathbb{Z}$ for $i = 1, \ldots, n$.*

PROOF. Since G is solvable, it has an abelian series. By Theorem 7.3 the abelian series and composition series have equivalent refinements. However, the composition series has only trivial refinements, so the factors in the composition series are all abelian and simple. Exercise 6.12 gives the desired conclusion. □

DEFINITION 8.4. Let G be a group. A *commutator* in G is an element of the form $xyx^{-1}y^{-1}$ for some $x, y \in G$. If X is the collection of commutators in G, then the *commutator subgroup* is $G^{(1)} = [G, G] = \langle X \rangle$.

An *automorphism* of G is an isomorphism $G \to G$.

THEOREM 8.5. *Let G be a group.*

(a) *If φ is an automorphism of G, then $\varphi([G, G]) = [G, G]$.*
(b) *$[G, G] \trianglelefteqslant G$.*
(c) *$G/[G, G]$ is abelian.*
(d) *G is abelian if and only if $[G, G] = \{e\}$.*

PROOF. (a) For $x, y \in G$, we have $\varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1}$. Hence, $\varphi(X) \subseteq X$, and it follows that $\varphi([G, G]) = \varphi(\langle X \rangle) \subseteq \langle X \rangle = [G, G]$.

Exercise 4(a) from assignment 3 shows that φ^{-1} is an automorphism of G, and so the previous paragraph implies $\varphi^{-1}([G, G]) \subseteq [G, G]$ and so

$$[G, G] = \varphi(\varphi^{-1}([G, G])) \subseteq \varphi([G, G]) \subseteq [G, G]$$

and hence $\varphi([G, G]) = [G, G]$.

(b) Fix an element $x \in G$. We need to show $x[G, G]x^{-1} = [G, G]$. Let $\phi_x \colon G \to G$ be given by $\phi_x(y) = xyx^{-1}$. Exercise 4(a) from assignment 3 shows that ϕ_x is an automorphism of G, and hence part (a) implies

$$x[G, G]x^{-1} = \phi_x([G, G]) = [G, G].$$

(c) For $\overline{x}, \overline{y} \in G/[G, G]$, we have

$$\overline{x}\ \overline{y}\ \overline{x}^{-1}\overline{y}^{-1} = \overline{xyx^{-1}y^{-1}} = \overline{e}$$

and so $\overline{x}\ \overline{y} = \overline{y}\ \overline{x}$.

(d) If G is abelian, then $xyx^{-1}y^{-1} = \{e\}$ for all $x, y \in G$ and so $[G, G] = \langle xyx^{-1}y^{-1} \rangle = \langle e \rangle = \{e\}$.

Conversely, if $[G, G] = \{e\}$, then $G/[G, G] = G/\{e\} \cong G$. Part (c) says that $G/[G, G]$ is abelian, so the isomorphism $G/[G, G] \cong G$ implies that G is abelian. □

9. Day 10

REMARK 9.1. We sometimes call $G/[G,G]$ the "abelianization" of G.

LEMMA 9.2 (Universal property for group quotients). *Let $f\colon G \to H$ be a homomorphism of groups, and let $K \trianglelefteq G$. TFAE.*

(i) *$K \subseteq \mathrm{Ker}(f)$;*
(ii) *The function $\overline{f}\colon G/K \to H$ given by $\overline{f}(\overline{g}) = f(g)$ is well-defined.*

When these conditions are satisfied, the map $\overline{f}$ is a group homomorphism.

PROOF. (i) $\Longrightarrow$ (ii) If $\overline{g} = \overline{h}$, then $gh^{-1} \in K \subseteq \mathrm{Ker}(f)$ and so

$$e_H = f(gh^{-1}) = f(g)f(h)^{-1}$$

which implies $f(g) = f(h)$.

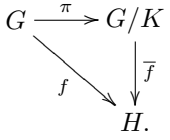
(ii) $\Longrightarrow$ (i) If $k \in K$, then $\overline{k} = \overline{e_G} \in G/K$ and so

$$f(k) = \overline{f}(\overline{k}) = \overline{f}(\overline{e_G}) = f(e_G) = e_H)$$

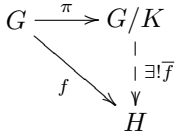
which implies $k \in \mathrm{Ker}(f)$.

It is straightforward to show that $\overline{f}$ is a group homomorphism. □

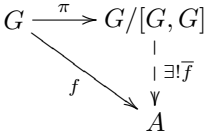
REMARK 9.3. Let $\pi\colon G \to G/K$ be the canonical epimorphism. In condition (ii) we say "f factors through π". In symbols, this mean $f = \overline{f}\pi$, in which case we say that the following diagram commutes



It is straightforward to show that $\overline{f}$ is the unique function g such that $f = g\pi$. A compact way to write the existence and uniqueness statements is with a dashed arrow.



THEOREM 9.4 (Universal property for the abelianization of a group). *Let G be a group, and let $\pi\colon G \to G/[G,G]$ be the canonical epimorphism. For each abelian group A and each group homomorphism $f\colon G \to A$ there exists a unique group homomorphism $\overline{f}\colon G/[G,G] \to A$ making the following diagram commute.*



PROOF. By Lemma 9.2 and Remark 9.3, it suffices to show $[G,G] \subseteq \mathrm{Ker}(f)$. For this, it suffices to show that, for each $x, y \in G$, we have $xyx^{-1}y^{-1} \in \mathrm{Ker}(f)$, which we show in the following computation:

$$\begin{aligned} f(xyx^{-1}y^{-1}) &= f(x)f(y)f(x)^{-1}f(y)^{-1} = f(y)f(x)f(x)^{-1}f(y)^{-1} \\ &= f(y)f(y)^{-1} = e_A. \end{aligned}$$

□

LEMMA 9.5. *If $H \trianglelefteq G$ such that G/H is abelian, then $[G,G] \subseteq H$.*

PROOF. Let $f\colon G \to G/H$ and $\pi\colon G \to G/[G,G]$ be the canonical epimorphisms. Because G/H is abelian, Theorem 9.4 implies that there exists a unique group homomorphism $\overline{f}\colon G/[G,G] \to G/H$ making the following diagram commute.

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/[G,G] \\ & \searrow^{f} & \downarrow \exists!\overline{f} \\ & & G/H. \end{array}$$

The fact that the diagram commutes says that $\overline{f}(\overline{g}) = f(g)$, so Lemma 9.2 implies $[G,G] \subseteq H$. □

DEFINITION 9.6. Set $G^{(0)} = G$. Recall that $G^{(1)} = [G,G]$. For $n \geqslant 2$, inductively define $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$.

REMARK 9.7. $G^{(n)} \trianglelefteq G^{(n-1)}$, and $G^{(n-1)}/G^{(n)}$ is abelian by Theorem 8.5.

THEOREM 9.8. *A group G is solvable if and only if $G^{(n)} = \{e\}$ for some n.*

PROOF. First assume that $G^{(n)} = \{e\}$ for some n. Then the sequence

$$\{e\} = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \cdots \trianglelefteq G^{(0)} = G$$

is normal abelian series, and so G is solvable.

Now, assume that G is solvable and let

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

be an abelian normal series. Assume without loss of generality that $G_i \neq G_{i-1}$ for each i.

Claim: $G^{(i)} \subseteq G_i$ for $i = 0, \ldots, n$. (Once this is shown, we are done since then $\{e\} \subseteq G^{(n)} \subseteq G_n = \{e\}$ implies $G^{(n)} = \{e\}$.)

Proof of claim: By induction. The case $i = 0$ is by definition: $G^{(0)} = G = G_0$. For the inductive step, assume $G^{(k)} \subseteq G_k$. Then we have

$$G^{(k+1)} = [G^{(k)}, G^{(k)}] \subseteq [G_k, G_k] \subseteq G_{k+1}.$$

The first containment is by definition. The second containment follows from the hypothesis $G^{(k)} \subseteq G_k$. The third containment is from Lemma 9.5. □

DEFINITION 9.9. G is *perfect* if $G^{(1)} = G$.

THEOREM 9.10. *If G is simple and non-abelian, then G is perfect.*

PROOF. We have $G^{(1)} \trianglelefteq G$. Since G is simple, this implies either $G^{(1)} = G$ or $G^{(1)} = \{e\}$. Because G is non-abelian, Theorem 8.5(d) implies $G^{(1)} \neq \{e\}$ and so $G^{(1)} = G$. □

10. Day 11

THEOREM 10.1. *Let $H \trianglelefteq G$ and let $\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$.*

(a) *We have $\{e\} = H \cap G_n \trianglelefteq H \cap G_{n-1} \trianglelefteq \cdots \trianglelefteq H \cap G_0 = H \cap G = H$ and $H \cap G_i \trianglelefteq G_i$ for all i.*
(b) *$(H \cap G_i)/(H \cap G_{i+1})$ is isomorphic to a normal subgroup of G_i/G_{i+1}.*
(c) *If G_i/G_{i+1} is simple, then $(H \cap G_i)/(H \cap G_{i+1})$ is simple or trivial.*
(d) *If G_i/G_{i+1} is abelian, then $(H \cap G_i)/(H \cap G_{i+1})$ is abelian.*

PROOF. (a) Argue as in Exercise 3.9(b) to show that $H \trianglelefteq G$ and $G_{i+1} \trianglelefteq G_i$ imply $H \cap G_{i+1} \trianglelefteq H \cap G_i \trianglelefteq G_i$.

(b) We have $H \cap G_i \trianglelefteq G_i$ by part (a), and we have $G_i \subseteq N_{G_{i+1}}$ because $G_{i+1} \trianglelefteq G_i$. Hence, Lemma 7.2 implies $(H \cap G_i)G_{i+1} \trianglelefteq G_iG_{i+1} = G_i$. Furthermore, Theorem 6.7(c) implies

$$\frac{H \cap G_i}{H \cap G_{i+1}} = \frac{H \cap G_i}{(H \cap G_i) \cap G_{i+1}} \cong \frac{(H \cap G_i)G_{i+1}}{G_{i+1}} \trianglelefteq \frac{G_i}{G_{i+1}}$$

where the last bit is from Theorem 6.10(b).

(c) and (d) From part (b). □

THEOREM 10.2. *Let $H \trianglelefteq G$ and let $\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$.*

(a) *$H \trianglelefteq G_iH$ for each i.*
(b) *$\{\overline{e}\} = (G_nH)/H \trianglelefteq (G_{n-1}H)/H \trianglelefteq \cdots \trianglelefteq (G_0H)/H = (GH)/H = G/H$.*
(c) *There exists a group epimorphism $F\colon G_i/G_{i+1} \to [(G_iH)/H]/[(G_{i+1}H)/H]$.*
(d) *If G_i/G_{i+1} is simple, then $[(G_iH)/H]/[(G_{i+1}H)/H]$ is simple or trivial.*
(e) *If G_i/G_{i+1} is abelian, then $[(G_iH)/H]/[(G_{i+1}H)/H]$ is abelian.*

PROOF. (a) We have $\{e\} \trianglelefteq G_i \subseteq N_H$ because $H \trianglelefteq G$. Thus, Lemma 7.2 implies $H = \{e\}H \trianglelefteq G_iH$.

(b) We have $G_{i+1} \trianglelefteq G_i \subseteq N_H$ because $H \trianglelefteq G$. Thus, Lemma 7.2 implies $G_{i+1}H \trianglelefteq G_iH$. Theorem 6.10(b) implies $(G_{i+1}H)/H \trianglelefteq (G_iH)/H$.

(c) Theorem 6.6(c) gives the first isomorphism in the next sequence

$$\frac{(G_iH)/H}{(G_{i+1}H)/H} \cong \frac{G_iH}{G_{i+1}H} = \frac{G_i(G_{i+1}H)}{G_{i+1}H} \cong \frac{G_i}{G_i \cap G_{i+1}H}.$$

The second isomorphism is from Theorem 6.7(c). This yields an isomorphism $h\colon G_i/(G_i \cap G_{i+1}H) \to [(G_iH)/H]/[(G_{i+1}H)/H]$.

We have $G_{i+1} \subseteq G_i \cap G_{i+1}H \subseteq G_i$, and $G_{i+1} \trianglelefteq G_i$. Hence, Lemma 9.2 implies that the function $f\colon G_i/G_{i+1} \to G_i/(G_i \cap G_{i+1}H)$ given by $\overline{g} \mapsto \overline{g}$ is a well-defined group homomorphism. This map is also clearly onto and hence is an epimorphism. It follows that the composition $F = hf\colon G_i/G_{i+1} \to [(G_iH)/H]/[(G_{i+1}H)/H]$ is a group epimorphism.

(d) Since G_i/G_{i+1} is simple and $\operatorname{Ker}(F) \trianglelefteq G_i/G_{i+1}$, we have either $\operatorname{Ker}(F) = G_i/G_{i+1}$ or $\operatorname{Ker}(F) = \{\overline{e}\}$. In either case, we have

$$G_i/(G_i \cap G_{i+1}H) = \operatorname{Im}(F) \cong (G_i/G_{i+1})/\operatorname{Ker}(F).$$

If $\operatorname{Ker}(F) = \{\overline{e}\}$, then

$$G_i/(G_i \cap G_{i+1}H) \cong (G_i/G_{i+1})/\operatorname{Ker}(F) = (G_i/G_{i+1})/\{\overline{e}\} \cong G_i/G_{i+1}$$

which is simple. If $\operatorname{Ker}(F) = G_i/G_{i+1}$, then

$$G_i/(G_i \cap G_{i+1}H) \cong (G_i/G_{i+1})/\operatorname{Ker}(F) = (G_i/G_{i+1})/(G_i/G_{i+1}) \cong \{e\}$$

which is trivial.

(e) Because G_i/G_{i+1} is abelian and F is an epimorphism, it follows that $[(G_iH)/H]/[(G_{i+1}H)/H]$ is abelian. □

THEOREM 10.3. *Let $H \trianglelefteq G$.*

(a) *G has a composition series if and only if H and G/H have composition series.*
(b) *G is solvable if and only if H and G/H are solvable.*

PROOF. (a) " $\Longleftarrow$ " Assume that H and G/H have composition series

$$\{e\} = H_n \trianglelefteq H_{n-1} \trianglelefteq \cdots \trianglelefteq H_0 = H$$
$$\{\overline{e}\} = K_m \trianglelefteq K_{m-1} \trianglelefteq \cdots \trianglelefteq K_0 = G/H$$

Theorem 6.10(b) implies that $K_1 = G_1/H$ for some $G_1 \trianglelefteq G$, and Theorem 6.6(c) implies

$$(G/H)/K_1 = (G/H)/(G_1/H) \cong G/G_1.$$

Hence, G/G_1 is simple or trivial. Similarly, $K_j = G_j/H$ for some $G_j \trianglelefteq G_{j-1}$, and G_{j-1}/G_j is simple or trivial. It follows that the concatenated series

$$\{e\} = H_n \trianglelefteq H_{n-1} \trianglelefteq \cdots \trianglelefteq H_0 = H = G_m \trianglelefteq G_{m-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

is a composition series for G.

" $\Longrightarrow$ " Assume that G has a composition series

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G.$$

Theorem 10.1(a) and (c) show that H has a composition series. Theorem 10.2(b) and (d) show that G/H has a composition series.

(b) is proved similarly. □

THEOREM 10.4. *If G is a finite group, then G has a composition series.*

PROOF. We proceed by strong induction on $n = |G|$. The case $n = 1$ is trivial.

Let $n > 1$ and assume that every finite group G' with $|G'| < n$ has a composition series. If G is simple, then the normal series $\{e\} \trianglelefteq G$ is a composition series. If G is not simple, then there is a normal subgroup $H \trianglelefteq G$ such that $H \neq \{e\}$ and $H \neq G$. Since $H \subsetneq G$, we have $|H| < |G| = n$, so H has a composition series by our induction hypothesis. On the other hand, Lagrange's theorem implies $|G/H| = |G|/|H| < |G| = n$ and so G/H also has a composition series by our induction hypothesis. Now apply Theorem 10.3(a). □

11. Day 12

Group actions.

DEFINITION 11.1. Let G be a group and S a set. A *(left) group action* of G on S is a function $\mu\colon G \times S \to S$ (written $gs = \mu(g, s)$) such that $g(hs) = (gh)s$ and $es = s$ for all $g, h \in G$ and all $s \in S$. When there is a group action of G on S, we say "G acts on S" or "S is a G-set".

Assume that G acts on S. The *orbit* of an element $s \in S$ is the set $\mathrm{orb}(s) = Gs = \{gs \in S \mid g \in G\} \subseteq S$. The *stabilizer* of an element $s \in S$ is the set $G_s = \{g \in G \mid gs = s\} \subseteq G$. Note that $G_s \leqslant G$ for all $s \in S$.

Group actions are everywhere.

EXAMPLE 11.2. S_n acts on $\{1, 2, \ldots, n\}$ by $\tau k = \tau(k)$

EXAMPLE 11.3. G acts on G by $gh = gh$.

EXAMPLE 11.4. G acts on G by conjugation: $g \cdot h = ghg^{-1}$. The orbit of h under this action is the *conjugacy class* of h and is denoted $C(h)$.

This can also be described in terms of the *conjugacy relation* on G: $h' \sim h$ if and only if $h' = ghg^{-1}$ for some $g \in G$. When $h \sim h'$ we say that h and h' are *conjugate*. This is an equivalence relation, and the equivalence class of h is exactly $C(h)$.

EXAMPLE 11.5. If $H \trianglelefteq G$, then G acts on H by conjugation: $g \cdot h = ghg^{-1}$.

EXAMPLE 11.6. If $S = \{\text{subgroups of } G\}$, then G acts on S by conjugation.

EXAMPLE 11.7. If $H \leqslant G$ and $G/H = \{\text{left cosets of } H \text{ in } G\}$, then G acts on G/H by $g(hH) = (gh)H$. (Note that we are not assuming $H \trianglelefteq G$.)

PROPOSITION 11.8. *If G acts on a set S, then there is a 1-1 correspondence $Gs \leftrightarrow G/G_s$ given by $gs \leftrightarrow gG_s$.*

PROOF. The following argument shows well-definedness and bijectivity of the correspondences: $gs = hs$ if and only if $s = g^{-1}hs$ if and only if $g^{-1}h \in G_s$ if and only if $hG_s = gG_s$. □

PROPOSITION 11.9. *If G is a finite group acting on a set S, then for all $s \in S$ we have $|Gs| \mid |G|$.*

PROOF. Proposition 11.8 implies $|Gs|$ is the number of distinct cosets of G_s in G. That is, $|Gs| = [G, G_s]$, and so Lagrange's Theorem says $|G| = |G_s|[G, G_s] = |G_s||Gs|$. □

DEFINITION 11.10. Let G be a group acting on sets S and S'. A function $\varphi\colon S \to S'$ is a *homomorphism of G-sets* or "preserves the action of G" if $\varphi(gs) = g\varphi(s)$ for all $g \in G$ and all $s \in S$. An *isomorphism of G-sets* is a bijective homomorphism of G-sets.

PROPOSITION 11.11. *Let S be a G-set and fix $s \in S$. There is an isomorphism of G-sets $\varphi\colon Gs \to G/G_s$ given by $gs \mapsto gG_s$.*

PROOF. Proposition 11.8 shows that φ is a well-defined bijection. We need to show that φ is a homomorphism of G-sets:

$$\varphi(g(g's)) = \varphi((gg')s) = (gg')G_s = g(g'G_s) = g\varphi(g's).$$

□

PROPOSITION 11.12. *If S is a G-set, then S is the disjoint union of its distinct orbits.*

PROOF. Since $es = s$ for all $s \in S$, we have $s \in Gs \subseteq \cup_{t \in S} Gt$, and so $S \subset \cup_{t \in S} Gt \subseteq S$ which implies $S = \cup_{t \in S} Gt$.

Claim: $Gs \cap Gs' \neq \emptyset \implies Gs = Gs'$. (This will complete the proof.) If $gs = g's'$, then for all $h \in G$, we have $hs = hg^{-1}gs = hg^{-1}g's' \in Gs'$. Hence, we have $Gs \subseteq Gs'$. By symmetry, we have $Gs' \subseteq Gs$ and so $Gs = Gs'$. □

THEOREM 11.13 (Class equation). *Let G be a finite group.*

(a) $|G| = \sum |C(g)|$ *where the sum is taken over all distinct conjugacy classes in* G.
(b) $|G| = |Z(G)| + \sum |C(g)|$ *where the sum is taken over all distinct conjugacy classes* $C(g) \neq \{g\}$ *in* G.

PROOF. (a) By Example 11.4 and Proposition 11.12, G is the disjoint union of its distinct conjugacy classes.

(b) From part (a) it suffices to show that $C(g) = \{g\}$ if and only if $g \in Z(g)$. If $C(g) = \{g\}$, then $hgh^{-1} = g$ for all $h \in G$ and so $g \in Z(G)$. The converse is even easier. □

DEFINITION 11.14. Let p be a prime number. A finite group G is a *p-group* if $|G| = p^n$ for some integer n.

COROLLARY 11.15. *If* $G \neq \{e\}$ *is a finite p-group, then* $Z(G) \neq \{e\}$.

PROOF. Suppose $Z(G) = \{e\}$. Each conjugacy class $C(g)$ is an orbit of a G-action on G. Hence, Proposition 11.11 and Lagrange's theorem imply $|C(g)| = |G/G_g| = [G, G_g] = |G|/|G_g| = p^{n_g}$ for some n_g. If $C(g) \neq \{g\}$, then $|C(g)| > 1$ and so $p \mid |C(g)|$. The class equation says $|G| = |Z(G)| + \sum |C(g)|$ where the sum is taken over all distinct conjugacy classes $C(g) \neq \{g\}$ in G and so

$$p^n = |G| = |Z(G)| + \sum |C(g)| = |Z(G)| + pk = 1 + pk$$

for some integer k. This is impossible. □

12. Day 13

DEFINITION 12.1. Let $H, K \leqslant G$ and set

$$[H, K] = \langle hkh^{-1}k^{-1} \mid h \in H \text{ and } k \in K \rangle.$$

Set $G_{(0)} = G$ and $G_{(1)} = G^{(1)}$. For $n \geqslant 2$, inductively define

$$G_{(n)} = [G, G_{(n-1)}] = \langle xyx^{-1}y^{-1} \mid x \in G \text{ and } y \in G_{(n-1)} \rangle.$$

G is *nilpotent* if $G_{(n)} = \{e\}$ for some n.

THEOREM 12.2. *Let* $H \leqslant G$. *Then* $[G, H] = \{e\}$ *if and only if* $H \subseteq Z(G)$. *In particular, if* $G \neq \{e\}$ *is nilpotent, then* $Z(G) \neq \{e\}$.

PROOF. Assume $H \subseteq Z(G)$. Then, for all $h \in H$ and all $g \in G$, we have $ghg^{-1}h^{-1} = e$ and so $[G, H] = \langle e \rangle = \{e\}$.

Assume $[G, H] = \{e\}$. Let $h \in H$. Then, for all and all $g \in G$, we have $ghg^{-1}h^{-1} \in [G, H] = \{e\}$ and so $ghg^{-1}h^{-1} = e$ and $gh = hg$. This holds for all $g \in G$, and so $h \in Z(G)$. This holds for all $h \in H$, and so $H \subseteq Z(G)$.

Assume G is nilpotent and let $m = \min\{n \geqslant 1 \mid G_{(n)} = \{e\}\}$. Then $\{e\} = G_{(m)} = [G, G_{(m-1)}]$ implies $\{e\} \neq G_{(m-1)} \subseteq Z(G)$. □

We'll see in an exercise that nilpotent implies solvable. The next example shows that the converse fails to hold in general.

EXAMPLE 12.3. S_3 is solvable by an exercise. But S_3 is not nilpotent because $Z(S_3) = \{(1)\}$.

If A is abelian, then $A_{(1)} = [A, A] = \{e\}$ and so A is nilpotent.

LEMMA 12.4. $G_{(n+1)} \subseteq G_{(n)} \trianglelefteq G$ *for all* $n \geqslant 0$, *and so* $G_{(n+1)} \trianglelefteq G_{(n)}$.

PROOF. By induction on n.
Base case $n = 0$: $G_{(1)} = [G, G] \subseteq G = G_{(0)}$.
Induction step. Assume $n \geqslant 0$ and $G_{(n+1)} \subseteq G_{(n)} \trianglelefteq G$. Then

$$G_{(n+2)} = [G, G_{(n+1)}] \subseteq [G, G_{(n)}] = G_{(n+1)}.$$

For $g \in G$ and $h \in G_{(n+1)}$ we have

$$ghg^{-1}h^{-1} \in [G, G_{(n+1)}]G_{(n+1)} = G_{(n+2)}G_{(n+1)} = G_{(n+1)}$$

and so $G_{(n+1)} \trianglelefteq G$. □

EXERCISE 12.5. If $\varphi\colon G \to H$ is a group epimorphism, then $\varphi(G^{(n)}) = H^{(n)}$ and $\varphi(G_{(n)}) = H_{(n)}$ for each $n \geqslant 0$. In other words, if $K \trianglelefteq G$, then $(G/K)^{(n)} = \{gK \in G/K \mid g \in G^{(n)}\}$ and $(G/K)_{(n)} = \{gK \in G/K \mid g \in G_{(n)}\}$.

The next result shows, in particular, that $G_{(n)}/G_{(n+1)}$ is abelian.

LEMMA 12.6. $G_{(n)}/G_{(n+1)} \subseteq Z(G/G_{(n+1)})$.

PROOF.

$$[G/G_{(n+1)}, G_{(n)}/G_{(n+1)}] = [G, G_{(n)}]/G_{(n+1)} = G_{(n+1)}/G_{(n+1)} = \{\overline{e}\}$$

and so Theorem 12.2 implies $G_{(n)}/G_{(n+1)} \subseteq Z(G/G_{(n+1)})$. □

DEFINITION 12.7. Let $Z_0(G) = \{e\}$ and for $k \geqslant 1$ let $Z_k(G)$ be the unique normal subgroup of G containing $Z_{k-1}(G)$ such that $Z_k(G)/Z_{k-1}(G) = Z(G/Z_{k-1}(G))$. This makes sense by Theorem 6.10(b) because $Z(G/Z_{k-1}(G)) \trianglelefteq G/Z_{k-1}(G)$.

REMARK 12.8. The construction of $Z_n(G)$ yields a "tower"

$$\{e\} = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \cdots$$

such that each quotient $Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G))$ is abelian. Lemmas 12.4 and 12.6 yield another "tower"

$$\cdots \trianglelefteq G_{(1)} \trianglelefteq G_{(0)} = G$$

such that the quotient $G_{(n)}/G_{(n+1)} \subseteq Z(G/G_{(n+1)})$ is abelian. We will see in Theorem 13.5 that the first tower terminates at G if and only if the second tower terminates at $\{e\}$.

LEMMA 12.9. *For $k, m \geqslant 0$, we have $Z_{k+m}(G)/Z_m(G) = Z_k(G/Z_m(G))$.*

PROOF. Use induction on k.
Base case, $k = 0$: $Z_0(G/Z_m(G)) = \{Z_m(G)\} = Z_m(G)/Z_m(G)$.
Base case, $k = 1$: $Z_1(G/Z_m(G)) = Z(G/Z_m(G)) = Z_{m+1}(G)/Z_m(G)$.

Inductive step: Assume $r \geqslant 1$ and $Z_{r+m}(G)/Z_m(G) = Z_r(G/Z_m(G))$ for all $m \geqslant 0$ and all groups G. Then

$$\begin{aligned}
\frac{Z_{r+1}(G/Z_m(G))}{Z_1(G/Z_m(G))} &= Z_r\left(\frac{G/Z_m(G)}{Z_1(G/Z_m(G))}\right) && \text{[inductive hypothesis]}\\
&= Z_r\left(\frac{G/Z_m(G)}{Z_{1+m}(G)/Z_m(G)}\right) && \text{[base case } k=1\text{]}\\
&\cong Z_r\left(\frac{G}{Z_{1+m}(G)}\right) && \text{[isomorphsim theorem]}\\
&= \frac{Z_{r+1+m}(G)}{Z_{1+m}(G)} && \text{[inductive hypothesis]}\\
&\cong \frac{Z_{r+1+m}(G)/Z_m(G)}{Z_{1+m}(G)/Z_m(G)} && \text{[isomorphsim theorem]}\\
&= \frac{Z_{r+1+m}(G)/Z_m(G)}{Z_1(G/Z_m(G))} && \text{[base case } k=1\text{]}.
\end{aligned}$$

Tracing through the isomorphisms, this gives

$$\frac{Z_{r+1}(G/Z_m(G))}{Z_1(G/Z_m(G))} = \frac{Z_{r+1+m}(G)/Z_m(G)}{Z_1(G/Z_m(G))}$$

and so Theorem 6.10(a) implies $Z_{r+1}(G/Z_m(G)) = Z_{r+1+m}(G)/Z_m(G)$. □

13. Day14

LEMMA 13.1. *If $G_{(n)} = \{e\}$ and $G_{(n-1)} \neq \{e\}$, then $G_{(n-j)} \subseteq Z_j(G)$ for $j = 0, \ldots, n$.*

PROOF. By induction on j.
Base case $j = 0$: $G_{(n)} = \{e\} = Z_0(G)$.
Induction step Assume $j \geqslant 0$ and $G_{(n-j)} \subseteq Z_j(G)$. Lemma 12.6 says

$$G_{(n-j-1)}/G_{(n-j)} \subseteq Z(G/G_{(n-j)})$$

and this yields the containment

$$\begin{aligned}
\frac{\langle G_{(n-j-1)}/G_{(n-j)}, Z_j(G)/G_{(n-j)}\rangle}{Z_j(G)/G_{(n-j)}} &\subseteq Z\left(\frac{G/G_{(n-j)}}{Z_j(G)/G_{(n-j)}}\right)\\
&\cong Z\left(\frac{G}{Z_j(G)}\right) && \text{[isomorphism theorem]}\\
&\cong \frac{Z_{j+1}(G)}{Z_j(G)} && \text{[definition]}\\
&\cong \frac{Z_{j+1}(G)/G_{(n-j)}}{Z_j(G)/G_{(n-j)}} && \text{[isomorphism theorem]}.
\end{aligned}$$

Tracing through the isomorphisms, we have

$$G_{(n-j-1)}/G_{(n-j)} \subseteq Z_{j+1}(G)/G_{(n-j)}$$

and so $G_{(n-j-1)} \subseteq Z_{j+1}(G)$. □

LEMMA 13.2. *If $G_{(n)} = \{e\}$ and $G_{(n-1)} \neq \{e\}$, then $Z_n(G) = G$ and $Z_j(G) \neq G$ for $j = 0, \ldots, n-1$.*

PROOF. By Lemma 13.1, we know $Z_n(G) = G$.
Set $n = n(G) = \min\{m \geqslant 0 \mid G_{(m)} = \{e\}\}$. We proceed by induction on $n(G)$.
Base case $n(G) = 0$: trivial.
Assume $n \geqslant 1$ and that the result holds for all groups H such that $n(H) < n$.
Claim: $n(G/Z(G)) < n$. Lemma 13.1 implies $G_{(n-1)} \subseteq Z_1(G) = Z(G)$, so

$$\begin{aligned}(G/Z(G))_{(n-1)} &= \{gZ(G) \in G/Z(G) \mid g \in G_{(n-1)}\} && \text{[Exercise 12.5]}\\ &= \{Z(G)\} && [G_{(n-1)} \subseteq Z(G)]\\ &= \{\overline{e}\}.\end{aligned}$$

This proves the claim.

Claim: $n(G/Z(G)) = n - 1$. It suffices to show that $j < n - 1$ implies $(G/Z(G))_{(j)} \neq \{\overline{e}\}$. (This is vacuous if $n = 1$.) Assume $j < n - 1$ and suppose $(G/Z(G))_{(j)} = \{\overline{e}\}$. Then

$$\{\overline{e}\} = (G/Z(G))_{(j)} = \{gZ(G) \in G/Z(G) \mid g \in G_{(j)}\}$$

implies $G_{(j)} \subseteq Z(G)$ and so $G_{(j+1)} = [G, G_{(j)}] = \{e\}$ by Theorem 12.2. This implies $j + 1 \geqslant n$ and so $j \geqslant n - 1$, a contradiction.

Now, our induction hypothesis applied to $G/Z(G)$ implies $Z_j(G/Z(G)) \neq G/Z(G)$ for all $j < n - 1$. Hence, Lemma 12.9 yields the second equality in the next sequence

$$G/Z(G) \neq Z_j(G/Z(G)) = Z_j(G/Z_1(G)) = Z_{j+1}(G)/Z_1(G) = Z_{j+1}(G)/Z(G)$$

and so $Z_{j+1}(G) \subsetneq G$ when $j < n - 1$. □

LEMMA 13.3. *If $Z_n(G) = G$ and $Z_{n-1} \neq G$, then $G_{(j)} \subseteq Z_{n-j}(G)$ for $j = 0, \ldots, n$.*

PROOF. By induction on j.
Base case $j = 0$: $G_{(0)} = G = Z_n(G)$.
Induction step. Assume $j \geqslant 0$ and $G_{(j)} \subseteq Z_{n-j}(G)$. By definition we have $Z_{n-j}(G)/Z_{n-j-1}(G) = Z(G/Z_{n-j-1}(G))$ and so

$$\begin{aligned}\{\overline{e}\} &= [G/Z_{n-j-1}(G), Z_{n-j}(G)/Z_{n-j-1}(G)]\\ &= \langle gzg^{-1}z^{-1}Z_{n-j-1}(G) \in G/Z_{n-j-1}(G) \mid g \in G, z \in Z_{n-j}(G)\rangle.\end{aligned}$$

It follows that all such $gzg^{-1}z^{-1}$ are in $Z_{n-j-1}(G)$, and so

$$Z_{n-j-1}(G) \supseteq [G, Z_{n-j}(G)] \supseteq [G, G_{(j)}] = G_{(j+1)}$$

as desired. □

LEMMA 13.4. *If $Z_n(G) = G$ and $Z_{n-1} \neq G$, then $G_{(n)} = \{e\}$ and $G_{(j)} \neq \{e\}$ for $j = 0, \ldots, n - 1$.*

PROOF. By Lemma 13.3, we know $G_{(n)} = \{e\}$. Let $j < n$ and suppose that $G_{(j)} = \{e\}$. Then Lemma 13.2 implies $Z_j(G) = G$ and hence $Z_{n-1}(G) = G$, a contradiction. Thus, we have $G_{(j)} \neq \{e\}$ for $j = 0, \ldots, n - 1$. □

THEOREM 13.5. *Let G be a group. $G_{(k)} = \{e\}$ if and only if $Z_k(G) = G$.*

PROOF. Lemmas 13.2 and 13.4. □

COROLLARY 13.6. *G is nilpotent if and only if $Z_k(G) = G$ for some k.*

PROOF. G is nilpotent if and only if $G_{(k)} = \{e\}$ for some k if and only if $Z_k(G) = G$ for some k. □

COROLLARY 13.7. *Every finite p-group G is nilpotent.*

PROOF. We need to show $Z_k(G) = G$ for some k. If $Z_1(G) = G$, then we're done. If $Z_1(G) \neq G$, then $p \leqslant |Z_1(G)| < |G| = p^n$. It follows that $G/Z_1(G)$ is a p-group of order less than p^n. By induction on $|G|$, we have

$$Z_k(G)/Z_1(G) = Z_{k-1}(G/Z_1(G)) = G/Z_1(G)$$

for some k, and so $Z_k(G) = G$. □

14. Day 15

Symmetric and alternating groups.

DEFINITION 14.1. Let $n \geqslant k \geqslant 1$. A *cycle of length k* or a *k-cycle* in S_n is an element of the form $(m_1\ m_2\ \dots\ m_k) \in S_n$. Two cycles $(m_1\ m_2\ \dots\ m_k)$ and $(m'_1\ m'_2\ \dots\ m'_{k'})$ in S_n are *disjoint* if $\{m_1, m_2, \dots, m_k\} \cap \{m'_1, m'_2, \dots, m'_{k'}\} = \emptyset$. If σ_1 and σ_2 are disjoint cycles, then $\sigma_1\sigma_2 = \sigma_2\sigma_1$. We say the number s *occurs* in the cycle $(m_1\ m_2\ \dots\ m_k)$ if $s = m_i$ for some i.

Every element $\sigma \in S_n$ has a *disjoint cycle decomposition*: There exist cycles $\sigma_1, \sigma_2, \cdots, \sigma_r \in S_n$ such that

(1) $\sigma = \sigma_1\sigma_2\cdots\sigma_r$;
(2) the cycles σ_i and σ_j are disjoint whenever $i \neq j$;
(3) each $s = 1, \dots, n$ occurs in (exactly) one of the σ_i.

Such a decomposition is unique up to the order of the factors.

REMARK 14.2. The proof of existence and uniqueness of disjoint cycle decompositions is a tedious exercise in bookkeeping. See Hungerford, p. 47, Theorem 6.3. It follows from the existence that S_n is generated by its cycles.

EXAMPLE 14.3. Compute a disjoint cycle decomposition for some $\sigma \in S_8$.

PROPOSITION 14.4. *Two elements in S_n are conjugate if and only if their disjoint cycle decompositions have the same number of k-cycles for each k.*

PROOF. ($\Longrightarrow$) Let $\sigma, \tau \in S_n$ where τ has disjoint cycle decomposition

$$\tau = (m_{1,1}\ m_{1,2}\ \dots\ m_{1,k_1})(m_{2,1}\ m_{2,2}\ \dots\ m_{2,k_2})\cdots(m_{r,1}\ m_{r,2}\ \dots\ m_{r,k_r}).$$

We claim that $\sigma\tau\sigma^{-1}$ has the following disjoint cycle decomposition:

$$\sigma\tau\sigma^{-1} = (\sigma(m_{1,1})\ \sigma(m_{1,2})\ \dots\ \sigma(m_{1,k_1}))\cdots(\sigma(m_{r,1})\ \sigma(m_{r,2})\ \dots\ \sigma(m_{r,k_r})).$$

This follows in part from the next computation:

$$\sigma\tau\sigma^{-1}(\sigma(k_{s,t})) = \sigma(\tau(k_{s,t})) = \begin{cases} \sigma(\tau(k_{s,t+1})) & \text{if } t < k_s \\ \sigma(\tau(k_{s,1})) & \text{if } t = k_s. \end{cases}$$

Furthermore, this decomposition is disjoint as σ is bijective: $\sigma(m_{i,j}) = \sigma(m_{i',j'})$ if and only if $m_{i,j} = m_{i',j'}$. It follows that the disjoint cycle decompositions of τ and $\sigma\tau\sigma^{-1}$ have exactly the same number of k-cycles for each k.

($\Longleftarrow$) Let $\sigma, \tau \in S_n$, and assume that the disjoint cycle decompositions of σ and τ have the same number of k-cycles for each k:

$$\tau = (m_{1,1}\ m_{1,2}\ \dots\ m_{1,k_1})(m_{2,1}\ m_{2,2}\ \dots\ m_{2,k_2})\cdots(m_{r,1}\ m_{r,2}\ \dots\ m_{r,k_r})$$
$$\sigma = (l_{1,1}\ l_{1,2}\ \dots\ l_{1,k_1})(l_{2,1}\ l_{2,2}\ \dots\ l_{2,k_2})\cdots(l_{r,1}\ l_{r,2}\ \dots\ l_{r,k_r}).$$

Define $\delta \in S_n$ by the formula $\delta(m_{i,j}) = l_{i,j}$. Because we have disjoint cycle decompositions, δ is a well defined bijection of $\{m_{1,1}, m_{1,2}, \dots m_{r,k_r}\} = \{1, 2, \dots, n\}$ to itself. Furthermore, the computation of the previous paragraph shows that $\sigma = \delta\tau\delta^{-1}$, so that σ and τ are conjugate. □

Corollary 14.5. *In S_4, let*

$$H = \{(1), (12)(34), (13)(24), (14)(23)\}.$$

Then $H \trianglelefteq S_4$.

Proof. Check by hand that $H \leqslant G$. Proposition 14.4 implies that $H = C((1\ 2)(3\ 4)) \cup \{(1)\}$, and furthermore that $\delta C((1\ 2)(3\ 4))\delta^{-1} = C((1\ 2)(3\ 4))$ and $\delta\{(1)\}\delta^{-1} = \{(1)\}$ for each $\delta \in S_4$. It follows that $\delta H \delta^{-1} = H$ for each $\delta \in S_4$, and so $H \trianglelefteq S_4$. □

Proposition 14.6. *S_n is generated by 2-cycles.*

Proof. We know that S_n is generated by its cycles, so we need to show that each cycle $(m_1\ m_2\ \dots\ m_k) \in S_n$ can be written as a product of cycles:

$$(m_1\ m_2\ \dots\ m_k) = (m_1\ m_2)(m_2\ m_3)\cdots(m_{k-1}\ m_k).$$

□

Proposition 14.7. *S_n is generated by 2-cycles of the form $(k\ k+1)$.*

Proof. By Proposition 14.6 it suffices to show that every 2-cycle $(l\ m)$ can be written as a product of 2-cycles of the form $(k\ k+1)$. Assume without loss of generality that $l < m$: otherwise rewrite $(l\ m) = (m\ l)$.

Proceed by induction on $m - l$. The case $m - l = 1$ is trivial, so assume that $m - l > 1$. Then

$$(l\ m) = (m-1\ m)(l\ m-1)(m-1\ m).$$

Our induction hypothesis implies that $(l\ m-1)$ can be written as a product of 2-cycles of the form $(k\ k+1)$, and so the display shows that the same is true of $(l\ m)$. □

Lemma 14.8. *Let $n \geqslant 5$, and let $H \trianglelefteq G \leqslant S_n$. If G contains all the 3-cycles of S_n and G/H is abelian, then H contains all the 3-cycles of S_n.*

Proof. For distinct $k_1, \dots, k_5$ between 1 and n, we have

$$\begin{aligned}(k_1\ k_2\ k_3) &= (k_1\ k_4\ k_3)(k_3\ k_2\ k_5)(k_1\ k_3\ k_4)(k_3\ k_5\ k_2)\\ &= (k_1\ k_4\ k_3)(k_2\ k_2\ k_5)(k_1\ k_4\ k_3)^{-1}(k_3\ k_5\ k_2)^{-1}\\ &\in [G, G]\\ &\subseteq H\end{aligned}$$

where the containment $\subseteq$ is because G/H is abelian; see Lemma 9.5. □

Theorem 14.9. *If $n \geqslant 5$, then S_n is not solvable.*

PROOF. Suppose that G is solvable and fix an abelian tower

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq G_1 \trianglelefteq G_0 = G.$$

By induction on i, Lemma 14.8 implies that each G_i contains all the 3-cycles, and so $(123) \in G_n$, a contradiction. □

15. Day 16

DEFINITION 15.1. Define an action of S_n on the polynomial ring $\mathbb{C}[X_1, \ldots, X_n]$ by the formula

$$(\sigma f)(X_1, \ldots, X_n) = f(X_{\sigma^{-1}(1)}, \ldots, X_{\sigma^{-1}(n)})$$

and set

$$F(X_1, \ldots, X_n) = \prod_{j<k}(X_j - X_k).$$

Then for $\sigma \in S_n$ we have

$$(\sigma F)(X_1, \ldots, X_n) = \prod_{j<k}(X_{\sigma^{-1}(j)} - X_{\sigma^{-1}(k)}) = \pm F(X_1, \ldots, X_n).$$

It follows that S_n acts on the set $\{F, -F\}$ in the same manner. Define the *alternating group* on n letters to be the stabilizer of F in S_n:

$$A_n = (S_n)_F = \{\sigma \in S_n \mid \sigma F = F\}.$$

THEOREM 15.2. *A_n is a subgroup of S_n such that $[S_n : A_n] = 2$, and so $A_n \trianglelefteq S_n$. Furthermore, A_n contains no 2-cycles.*

PROOF. Since A_n is the stabilizer of a group action, it follows that $A_n \leqslant S_n$; see Definition 11.1. Furthermore, Proposition 11.8 implies

$$[S_n : A_n] = |S_n/A_n| = |S_n\{F\}| = |\{F, -F\}| = 2$$

and it follows from an exercise that $A_n \trianglelefteq S_n$.

One checks readily that $(1\ 2)F = -F$ and so $(1\ 2) \notin A_n$. For each $(l\ m)$ such that $l \neq m$, we know that $(l\ m)$ is conjugate to $(1\ 2)$ by Proposition 14.4. Since $(1\ 2) \notin A_n \trianglelefteq S_n$, it follows that $(l\ m) \notin A_n$. □

THEOREM 15.3. *Let $n \geqslant 2$.*

(a) *Let $\sigma \in S_n$ and let $\sigma = \tau_1 \cdots \tau_r = \pi_1 \cdots \pi_s$ where each τ_i and π_j is a 2-cycle. Then r and s have the same parity, that is, r is even if and only if s is even.*
(b) *$\sigma \in A_n$ if and only if σ is a product of an even number of 2-cycles.*
(c) *A_n is generated by the set of products of two 2-cycles.*
(d) *A_n is generated by $\{$products of two disjoint 2-cycles$\} \cup \{$3-cycles$\}$.*

PROOF. (a) Proposition 14.6 shows that σ can be written as a product of 2-cycles. Theorem 15.2 implies $\tau_i F = -F = \pi_j F$ for each i, and so

$$\sigma F = \tau_1 \cdots \tau_r F = (-1)^r F$$

and similarly, $\sigma F = (-1)^s F$. Hence, $(-1)^r = (-1)^s$ and so r and s have the same parity.

(b) $\sigma \in A_n$ if and only if $\sigma F = F$. Hence the proof of part (a) shows that $\sigma \in A_n$ if and only if $(-1)^r F = F$ if and only if r is even.

Part (c) now follows. Part (d) also follows because each product of two 2-cycles is either disjoint, or a 3-cycle, or the identity. □

LEMMA 15.4. *Let $n \geqslant 5$, and let $\{(1)\} \neq N \trianglelefteq A_n$. If $\sigma \in N$ such that σ moves five or more elements, then there exists $\delta \in N$ such that $\delta \neq (1)$ and δ moves fewer elements than σ.*

PROOF. Let $\sigma = \tau_1 \cdots \tau_k$ be a decomposition into disjoint cycles.

Case 1: τ_j is an s-cycle for some j and some $s \geqslant 5$, say $\tau_j = (m_1\ m_2\ \ldots\ m_s)$. Set $\gamma_j = (m_2\ m_1\ m_3\ \ldots\ m_{s-2}\ m_s\ m_{s-1})$, and for $r \neq j$ set $\gamma_r = \tau_r$. It follows that the permutation

$$\alpha = \gamma_1 \cdots \gamma_k = (m_1\ m_2)(m_{s-1}\ m_s)\sigma(m_1\ m_2)(m_{s-1}\ m_s) \in N$$

because $(m_1\ m_2)(m_{s-1}\ m_s) \in A_n$ and $\sigma \in N \trianglelefteq A_n$. The element $\delta = \sigma\alpha \in N$ satisfies the desired conditions:

First, $\delta(m_1) = \sigma(\alpha(m_1)) = \sigma(m_3) = m_4$ and so $\delta \neq (1)$.

Also, $\delta(m_2) = \sigma(\alpha(m_2)) = \sigma(m_1) = m_2$. By construction, δ only differs from σ by what happens to $m_1, \ldots, m_s$. Also, σ moves each $m_1, \ldots, m_s$. Hence, it follows that δ moves fewer elements than σ.

Case 2: τ_j is a 4-cycle for some j, say $\tau_j = (m_1\ m_2\ m_3\ m_4)$. Set $\gamma_j = (m_1\ m_3\ m_4\ m_2)$, and for $r \neq j$ set $\gamma_r = \tau_r$. As above, it follows that

$$\alpha = \gamma_1 \cdots \gamma_k = (m_3\ m_4\ m_2)\sigma(m_3\ m_2\ m_4) \in N$$

and the element $\delta = \sigma\alpha \in N$ satisfies the desired conditions.

Case 3: Each τ_r has length $\leqslant 3$, and two distinct τ_r have length 3. Since the τ_r are disjoint, assume that $\tau_1 = (m_1\ m_2\ m_3)$ and $\tau_2 = (m_4\ m_5\ m_6)$. Set $\gamma_1 = (m_1\ m_2\ m_4)$ and $\gamma_2 = (m_3\ m_6\ m_5)$, and for $r > 2$ set $\gamma_r = \tau_r$. As above, set $\alpha = \gamma_1 \cdots \gamma_k$, and the element $\delta = \sigma\alpha \in N$ satisfies the desired conditions.

Case 4: Each τ_r has length $\leqslant 3$, and there is a unique τ_j of length 3, say $\tau_1 = (m_1\ m_2\ m_3)$. Since σ moves at least five elements and each $\tau_r \neq \tau_1$ is a 2-cycle and $\sigma \in A_n$, we know that σ contains at least two 2-cycles: say $\tau_2 = (m_4\ m_5)$ and $\tau_3 = (m_6\ m_7)$. Set $\gamma_1 = (m_1\ m_3\ m_2)$ and $\gamma_2 = (m_4\ m_6)$ and $\gamma_3 = (m_5\ m_7)$, and for $r > 3$ set $\gamma_r = \tau_r$. As above, set $\alpha = \gamma_1 \cdots \gamma_k$, and the element $\delta = \sigma\alpha \in N$ satisfies the desired conditions.

Case 5: Each τ_r has length $\leqslant 2$. Since σ moves at least five elements, we know $k \geqslant 3$. Since $\sigma \in A_n$, Theorem 15.3 implies $k \geqslant 4$, say $\tau_1 = (m_1\ m_2)$, $\tau_2 = (m_3\ m_4)$, $\tau_3 = (m_5\ m_6)$, and $\tau_4 = (m_7\ m_8)$. Set $\alpha = (m_1\ m_2\ m_3)\sigma(m_1\ m_3\ m_2)$, and the element $\delta = \sigma\alpha \in N$ satisfies the desired conditions. □

LEMMA 15.5. *Let $n \geqslant 5$, and let $\{(1)\} \neq N \trianglelefteq A_n$. Then N contains either a 3-cycle or a disjoint product of two 2-cycles.*

PROOF. By repeated application of Lemma 15.4 we see that N contains a permutation $\sigma \neq (1)$ that moves at most four elements. It follows that σ is either a 2-cycle, a 3-cycle, a 4-cycle, or a disjoint product of two 2-cycles. Since σ is in A_n, Theorem 15.3 implies that σ is a 3-cycle or a disjoint product of two 2-cycles. □

THEOREM 15.6. *If $n \geqslant 5$, then A_n is simple.*

PROOF. Assume $\{(1)\} \neq N \trianglelefteq A_n$. We want to prove $N = A_n$. By Lemma 15.5, we have two cases.

Case 1: N contains a 3-cycle $(m_1\ m_2\ m_3) \in N$. Since $n \geqslant 5$ we can choose $m_4, m_5 \leqslant n$ distinct from m_1, m_2, m_3.

Claim (a): N contains all 3-cycles $\tau \in S_n$. Proof: Proposition 14.4 implies that $\tau = \sigma(m_1\ m_2\ m_3)\sigma^{-1}$ for some $\sigma \in S_n$. If $\sigma \in A_n$, then $\tau \in N$ because $N \trianglelefteqslant A_n$. If $\sigma \notin A_n$, then $\sigma(m_4\ m_5) \in A_n$, and so

$$\begin{aligned}\tau &= \sigma(m_1\ m_2\ m_3)\sigma^{-1}\\ &= \sigma(m_4\ m_5)(m_4\ m_5)(m_1\ m_2\ m_3)\sigma^{-1}\\ &= \sigma(m_4\ m_5)(m_1\ m_2\ m_3)(m_4\ m_5)\sigma^{-1}\\ &= (\sigma(m_4\ m_5))(m_1\ m_2\ m_3)(\sigma(m_4\ m_5))^{-1}\\ &\in N.\end{aligned}$$

This proves the claim.

Claim (b): N contains all disjoint products of two 2-cycles. Proof: If m_1, m_2, m_3, m_4 are distinct, then the previous claim implies

$$(m_1\ m_2)(m_3\ m_4) = (m_1\ m_2\ m_3)(m_2\ m_3\ m_4) \in N.$$

Now, Theorem 15.3 says that A_n is generated by the set of all products of two 2-cycles. This says that A_n is generated by

$$X = \{\text{disjoint products of two 2-cycles in } S_n\} \cup \{\text{all 3-cycles in } S_n\}$$

Our two claims show $X \subseteq N$ and so $A_n = \langle X\rangle \subseteq N \subseteq A_n$. This concludes the proof for case 1.

Case 2: N contains a disjoint product of two 2-cycles $(m_1\ m_2)(m_3\ m_4) \in N$. The proof of Claim (a) above shows that N contains every disjoint product of two 2-cycles. In particular,

$$(1\ 5\ 2) = (1\ 2)(3\ 4)(3\ 4)(1\ 5) \in N$$

and we are done by Case 1. □

16. Day 17

Sylow Theorems.

Definition 16.1. Let G be a finite group. Let p be a (positive) prime number, and write $|G| = p^n m$ where $p \nmid m$. A *p-Sylow subgroup* or *Sylow p-subgroup* of G is a subgroup $H \leqslant G$ such that $|H| = p^n$.

Definition 16.2. The *order* of an element $g \in G$ is

$$|g| = |\langle g\rangle| = \inf\{n \geqslant 1 \mid g^n = e\}.$$

In other words, $|g| = \infty$ if $g^n \neq e$ for all $n \geqslant 1$, and $|g| = m < \infty$ if $g^m = e$ and $g^n \neq e$ when $1 \leqslant n < m$.

If $|G| < \infty$, then $|g| < \infty$ for all $g \in G$, and Lagrange's Theorem implies $|g| \mid |G|$ and moreover $|G/\langle g\rangle| = |G|/|g|$.

If $|G| = \infty$, then G may contain elements of finite order and elements of infinite order, e.g., if $G = \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Lemma 16.3. *If G is a finite abelian group and p is a positive prime number such that $p \mid |G|$, then G contains an element of order p.*

PROOF. Proof by induction on $|G|/p$.

Base case: $|G|/p = 1$. Then $|G| = p$ and so $G \cong \mathbb{Z}/p\mathbb{Z}$. Thus, any generator of G has order p.

Induction step: Assume the result holds for all finite groups G' such that $p \mid |G'|$ and $|G'|/p < |G|/p$. Fix $e \neq g \in G$. If $p \mid |g|$, then $g^{|g|/p}$ has order p. So, assume $p \nmid |g|$. Then $p \mid |G|/|g| = |G/\langle g\rangle|$. Also, $g \neq e \implies |G/\langle g\rangle| < |G|$, and so $|G/\langle g\rangle|/p < |G|/p$. The induction hypothesis implies that there exists an element $h \in G$ such that $\overline{h} \in G/\langle g\rangle$ has order p. Lagrange's Theorem can be used to show $p = |\overline{h}| \mid |h|$. Hence, $h^{|h|/p}$ has order p. □

THEOREM 16.4 (Sylow Theorem I). *If G is a finite group and p is a positive prime number, then G has a p-Sylow subgroup $P \leqslant G$.*

PROOF. Write $|G| = p^n m$ where $p \nmid m$.

Step 0. If $n = 0$, then $P = \{e\}$ works. If $m = 1$, then $P = G$ works.

Step 1. G is cyclic, say, $G = \langle a\rangle$. Then the subgroup $P = \langle a^m\rangle$ works.

Step 2. We prove the result by induction on $|G|/p$. The base case $|G|/p = 1$ follows from Step 0.

Induction step: Assume the result holds for all finite groups G' such that $p \mid |G'|$ and $|G'|/p < |G|/p$. If G has a proper subgroup $H < G$ such that $p^n \mid |H|$, then the induction hypothesis implies that H has a subgroup P such that $|P| = p^n$; then H is also a p-Sylow subgroup of G. So, assume that $p^n \nmid |H|$ for all proper subgroups $H < G$. Lagrange's Theorem implies that $p \mid [G : H]$ for all proper subgroups $H < G$, and so $p \mid [G : Z_g]$ for all $g \in G - Z(G)$. Recall that Z_g is the centralizer of g from 6.3. This is exactly the stabilizer G_g of g under the conjugation action. Hence, Proposition 11.8 implies

$$[G : Z_g] = [G : G_g] = |G/G_g| = |\operatorname{orb}_G(g)| = |C(g)|.$$

It follows that $p \mid |C(g)|$ for all $g \in G \smallsetminus Z(G)$. Hence, the Class Equation 11.13(b) implies $p \mid |Z(G)|$. Lemma 16.3 yields an element $g \in Z(G)$ of order p. Hence, we have $\{e\} \neq \langle g\rangle \trianglelefteq G$. Since $|\langle g\rangle| = p$, Lagrange's Theorem implies $|G/\langle g\rangle| = p^{n-1}m$. Hence, the induction hypothesis provides a subgroup $H \leqslant G/\langle g\rangle$ of order p^{n-1}. (Unless $n = 1$, in which case we can use $H = \{\overline{e}\}$.) Then $H = P/\langle g\rangle$ for some subgroup $P \leqslant G$ containing g. Finally, Lagrange's Theorem implies $|P| = |H||\langle g\rangle| = p^n$. □

THEOREM 16.5 (Sylow Theorem). *Let G be a finite group, and let P be a p-Sylow subgroup of G. Then a subgroup $Q \leqslant G$ is a p-Sylow subgroup of G if and only if Q is conjugate to P.*

PROOF. ($\Longleftarrow$) If Q is conjugate to P, then $|Q| = |P|$, and so Q is a p-Sylow subgroup of G.

($\Longrightarrow$) Assume that Q is a p-Sylow subgroup of G, and let S denote the set of conjugates of P. Then G and Q both act on S by conjugation. We need to show $Q \in S$.

Claim: There exists an element $P' \in S$ such that $Q \subseteq N_{P'}$. Proof of claim: Proposition 11.8 shows $S = \operatorname{orb}_G(P) \leftrightarrow G/G_P = G/N_P$. Hence, we have $|S| = [G : N_P]$, and since $P \subseteq N_P$ we know that $p \nmid |S|$. However, since Q acts on S, Proposition 11.8 shows that $\operatorname{orb}_Q(P') \leftrightarrow Q/Q_{P'}$, and so every Q-orbit in S has either 1 element or the number of elements is divisible by p by Lagrange's Theorem. Since S is the disjoint union of its Q-orbits, we see that there exists an element

$P' \in S$ such that the Q-orbit of P' has exactly one element, namely P'. Hence, $Q \subseteq N_{P'}$.

From Theorem 5.5 we have $Q \leqslant QP' \leqslant G$, and Theorem 5.7 implies $|QP'| = |Q||P'|/|Q \cap P'|$. It follows that

$$p^n \mid |QP'| \mid |Q||P'| = p^{2n}.$$

Hence $|QP'| = p^k$ for some $n \leqslant k \leqslant 2n$. However, $QP' \leqslant G$ implies $|QP'| \mid |G| = p^n m$; since $\gcd(m, p) = 1$, we have $|QP'| = p^n$. We have $Q \subseteq QP'$ and $|Q| = p^n = |QP'|$, and so $Q = QP'$. Also, we have $P' \subseteq QP' = Q$ and $|P'| = p^n = |Q|$, and so $Q = P' \in S$, and we are done. □

17. Days 18 and 19

THEOREM 17.1 (Sylow Theorem III). *Let G be a finite group and p a positive prime number. Write $|G| = p^n m$ where $p \nmid m$, and let r be the number of p-Sylow subgroups of G. Then $r \equiv 1 \pmod{p}$ and $r \big| m$.*

PROOF. Let P be a fixed p-Sylow subgroup of G and let S denote the set of conjugates of P, that is, S is the set of all p-Sylow subgroups of G. Let P act on S by conjugation.

Claim: P is the unique fixed point in S under this action. In other words, for each $a \in G$, we have $b(aPa^{-1})b^{-1} = aPa^{-1}$ for all $b \in P$ if and only if $aPa^{-1} = P$.

Proof of claim: ($\Longleftarrow$) If $aPa^{-1} = P$, then, for all $b \in P$ we have $b(aPa^{-1})b^{-1} = bPb^{-1} = P = aPa^{-1}$. ($\Longrightarrow$) Assume $b(aPa^{-1})b^{-1} = aPa^{-1}$ for all $b \in P$. Then $P \subseteq N_{aPa^{-1}}$ and so the argument of Theorem 16.5 implies $P = aPa^{-1}$. This proves the claim.

Since S is the disjoint union of its orbits, we have

$$r = 1 + \sum |\operatorname{orb}_P(Q)|$$

where the sum is taken over all distinct P-orbits $\operatorname{orb}_P(Q) \neq \{P\}$. Proposition 11.8 shows $|\operatorname{orb}_P(Q)| = [P : P_Q]$, and so $p \big| |\operatorname{orb}_P(Q)|$ for each $\operatorname{orb}_P(Q) \neq \{P\}$. The displayed equation shows $r = 1 + pk$ for some k, and so $r \equiv 1 \pmod{p}$.

Letting G act on S, we have $S = \operatorname{orb}_G(P)$ and so

$$r = |\operatorname{orb}_G(P)| = [G : G_P] \big| |G|. = p^n m.$$

The congruence $r \equiv 1 \pmod{p}$ implies $\gcd(r, p) = 1$ and so $r \big| m$. □

THEOREM 17.2. *If G is a finite group and $H \leqslant G$ is a p-subgroup, then there exists a p-sylow subgroup $P \leqslant G$ such that $H \leqslant P$.*

PROOF. Let S be the set of p-sylow subgroups of G and let H act on S by conjugation. There is at least one fixed point under this action, call it P. (If there is no fixed point, then the proof of Theorem 17.1 shows $p \big| |\operatorname{orb}_H(Q)|$ for each $Q \in S$ and so $p \big| |S| = 1 + pk$; contradiction.) It follows that $H \leqslant N_P$ and so $HP \leqslant G$. As in the proof of Theorem 16.5 we have $HP = P$, and so $H \subseteq HP = P$. □

The next result generalizes one of our favorite exercises: If $H \leqslant G$ and $[G : H] = 2$, then $H \trianglelefteqslant G$.

PROPOSITION 17.3. *Let $G \neq \{e\}$ be a finite group, and let p be the smallest positive prime number dividing $|G|$. If $H \leqslant G$ and $[G : H] = p$, then $H \trianglelefteqslant G$.*

PROOF. Suppose that H is not a normal subgroup of G. Let S be the set of conjugates of H in G, and let $\mathrm{Perm}(S)$ denote the set of permutations of S. For all $g \in G$, let $\phi_g \colon S \to S$ be given by $K \mapsto gKg^{-1}$. It is routine to show that each $\phi_g \in \mathrm{Perm}(S)$ and that the map $\phi \colon G \to \mathrm{Perm}(S)$ given by $g \mapsto \phi_g$ is a group homomorphism.

Proposition 11.8 shows $|S| = [G : N_H]$. Since $H \subseteq N_H$, we have $p = [G : H] \geqslant [G : N_H]$. Because $[G : N_H] \big| |G|$, this implies $[G : N_H] = 1$ or $[G : N_H] = p$. Since H is not a normal subgroup of G, we have $N_H \neq G$; hence

$$p = [G : N_H] \leqslant [G : H] = p$$

and so $|S| = [G : N_H] = p$. Thus, there is an isomorphism $\Psi \colon \mathrm{Perm}(S) \to S_p$.

The equality $p = [G : N_H] = [G : H]$ implies $N_H = H$. It follows that, for all $g \in G - H$ we have $gHg^{-1} \neq H$. In particular, for all $g \in G - H$ we have $\phi_g \neq \mathrm{id}_S$ and so $\mathrm{Ker}(\phi) \subseteq H$.

Claim: $\mathrm{Ker}(\phi) = H$. Suppose not. Then $\mathrm{Ker}(\phi) \subsetneq H$, and so

$$[G : \mathrm{Ker}(\phi)] = [G : H][H : \mathrm{Ker}(\phi)] = p[H : \mathrm{Ker}(\phi)].$$

The composition $\Psi\phi \colon G \to S_p$ shows that the group $G/\mathrm{Ker}(\phi) = G/\mathrm{Ker}(\Psi\phi)$ is isomorphic to $\mathrm{Im}(\Psi\phi) \leqslant S_p$. In particular, we have

$$p[H : \mathrm{Ker}(\phi)] = [G : \mathrm{Ker}(\phi)] = |G/\mathrm{Ker}(\phi)| \big| |S_p| = p!.$$

It follows that $[H : \mathrm{Ker}(\phi)] \big| (p-1)!$. Since $[H : \mathrm{Ker}(\phi)] \neq 1$, there is a prime $q < p$ such that $q \big| [H : \mathrm{Ker}(\phi)] \big| G$. It follows that $q \big| |G|$, contradicting the minimality of p.

It follows that $H = \mathrm{Ker}(\phi) \trianglelefteq G$, a contradiction. □

The next result generalizes Lemma 16.3.

PROPOSITION 17.4. *If G is a finite group and p is a prime number such that $p \big| |G|$, then G contains an element of order p.*

PROOF. Let $P \leqslant G$ be a p-Sylow subgroup. By Corollary 11.15, we know $Z(P) \neq \{e\}$. Lagrange's Theorem implies $|Z(P)| \big| |P| = p^k$, and so the condition $|Z(P)| > 1$ implies $p \big| |Z(P)|$. Lemma 16.3 shows that $Z(P)$ contains an element of order p, and this is an element of G of order p. □

PROPOSITION 17.5. *Let N and H be normal subgroups of a finite group G. If $\gcd(|N|, |H|) = 1$, then $nh = hn$ for all $n \in N$ and all $h \in H$.*

PROOF. For all $n \in N$ and all $h \in H$, we have $nhn^{-1} \in H$ because $H \trianglelefteq G$, and so $nhn^{-1}h^{-1} \in H$. Lagrange's Theorem implies $|nhn^{-1}h^{-1}| \big| |H|$. Similarly, $hn^{-1}h^{-1} \in N \implies nhn^{-1}h^{-1} \in N \implies |nhn^{-1}h^{-1}| \big| |N|$. It follows that $|nhn^{-1}h^{-1}| \big| \gcd(|N|, |H|) = 1$, and so $nhn^{-1}h^{-1} = e$. □

PROPOSITION 17.6. *Let p and q be prime numbers such that $1 < p < q$ and $|G| = pq$. Let s denote the number of p-Sylow subgroups of G.*

(a) *There is a homorphism $\psi \colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ such that $G \cong \mathbb{Z}/q\mathbb{Z} \times_\psi \mathbb{Z}/p\mathbb{Z}$.*
(b) *If $s \neq q$, then $G \cong \mathbb{Z}/(pq)\mathbb{Z}$.*

PROOF. (a) Let $P \leqslant G$ be a p-Sylow subgroup, and let $Q \leqslant G$ be a q-Sylow subgroup. Since $|P| = p$, we have $P \cong \mathbb{Z}/p\mathbb{Z}$, and similarly we have $Q \cong \mathbb{Z}/q\mathbb{Z}$. In particular, every nonidentity element of P has order p, and every nonidentity

element of Q has order q. Because p and q are distinct primes, it follows that $P \cap Q = \{e\}$.

Since $[G, Q] = p$ and p is the smallest prime number dividing $|G|$, Proposition 17.3 implies $Q \trianglelefteq G$. In particular, $P \subseteq N_Q$ and so $PQ \leqslant G$. Moreover,

$$|PQ| = |P||Q|/|P \cap Q| = |P||Q| = pq = |G|$$

and so $G = PQ$.

Since $Q \trianglelefteq G$ an exercise yields the following. For each $x \in P$ the map $\phi_x \colon Q \to Q$ given by $y \mapsto xyx^{-1}$ is a well-defined automorphism of Q. The assignment $\phi(x) = \phi_x$ describes a homorphism $\phi \colon P \to \mathrm{Aut}(Q)$, and $G \cong Q \times_\phi P$. The isomorphisms $P \cong \mathbb{Z}/p\mathbb{Z}$ and $Q \cong \mathbb{Z}/q\mathbb{Z}$ yield the desired conclusion.

(b) Theorem 17.1 implies

$$s \big| |G|/|P| = pq/p = q.$$

Since $s \neq q$, we have $s = 1$. Hence $P \trianglelefteq G$, and Proposition 17.5 implies $xy = yx$ for all $x \in P$ and all $y \in Q$. In particular, the homomorphism ϕ from the proof of part (a) satisfies $\phi_x = \mathrm{id}_Q$ for all x. The exercise on semi-direct products implies

$$G \cong Q \times_\phi P \cong Q \times P \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/(pq)\mathbb{Z}$$

where the last isomorphism follows from the fact that $\gcd(p, q) = 1$. □

Structure theorems for finitely generated abelian groups.

REMARK 17.7. When G is an abelian group, we will use additive notation for the operation. Hence, we write $g + h$ instead of gh for the operation, $-g$ instead of g^{-1} for the inverse of g, 0 instead of e for the identity in G, and ng instead of g^n when $n \in \mathbb{Z}$.

DEFINITION 17.8. Let $\{G_\alpha\}_{\alpha \in A}$ be a set of abelian groups. The *product* $\prod_{\alpha \in A} G_\alpha$ is the cartesian product with operation defined coordinatewise. In other words,

$$\prod_{\alpha \in A} G_\alpha = \{\text{sequences } (g_\alpha) \text{ such that } g_\alpha \in G_\alpha \text{ for each } \alpha \in A\}$$
$$(g_\alpha) + (h_\alpha) = (g_\alpha + h_\alpha)$$
$$-(g_\alpha) = (-g_\alpha)$$
$$0_{\prod_{\alpha \in A} G_\alpha} = (0_{G_\alpha})$$

These operations are well-defined and endow $\prod_{\alpha \in A} G_\alpha$ with the structure of an abelian group. The *direct sum* is the subgroup

$$\oplus_{\alpha \in A} G_\alpha = \{(g_\alpha) \in \textstyle\prod_{\alpha \in A} G_\alpha \mid g_\alpha = 0 \text{ for all but finitely many } \alpha \in A\} \leqslant \prod_{\alpha \in A} G_\alpha.$$

If $A = \emptyset$, then $\prod_{\alpha \in \emptyset} G_\alpha = \oplus_{\alpha \in \emptyset} G_\alpha = \{0\}$. If A is finite, then $\prod_{\alpha \in A} G_\alpha = \oplus_{\alpha \in A} G_\alpha$.

18. Day 20

DEFINITION 18.1. Let G be an abelian group and $\{G_\alpha\}_{\alpha \in A}$ a set of subgroups of G. Set $\sum_{\alpha \in A} G_\alpha = \langle \cup_{\alpha \in A} G_\alpha \rangle \leqslant G$.

PROPOSITION 18.2. *Let G be an abelian group and $\{G_\alpha\}_{\alpha \in A}$ a set of subgroups of G. Assume that $G = \sum_{\alpha \in A} G_\alpha$. Assume that, for all $n \in \mathbb{N}$ and all distinct elements $\alpha_0, \alpha_1, \ldots, \alpha_n \in A$ we have $G_{\alpha_0} \cap \sum_{i=1}^n G_{\alpha_i} = \{0\}$. Then $G \cong \oplus_{\alpha \in A} G_\alpha$.*

PROOF. Define $\varphi\colon \oplus_{\alpha\in A} G_\alpha \to G$ by the formula $\varphi((g_\alpha)) = \sum_\alpha g_\alpha$. The fact that only finitely many of the g_α are nonzero says that the sum is finite. Check that this is a well-defined abelian group homomorphism.

φ is surjective: Let $g \in G$. The assumption $G = \sum_{\alpha\in A} G_\alpha$ implies that there exist $n \in \mathbb{N}$ and $\alpha_1, \dots, \alpha_n \in A$ and $g_{\alpha_i} \in G_{\alpha_i}$ such that $g = \sum_i g_{\alpha_i}$. For $\alpha \in A$ such that $\alpha \notin \{\alpha_1, \dots, \alpha_n\}$ set $g_\alpha = 0$. It follows that

$$\varphi((g_\alpha)) = \textstyle\sum_\alpha g_\alpha = \sum_i g_{\alpha_i} = g$$

and so φ is surjective.

φ is injective: Let $(g_\alpha) \in \operatorname{Ker}(\varphi)$ and suppose $(g_\alpha) \neq (0)$. Let $g_{\alpha_0}, \dots, g_{\alpha_n}$ be the distinct nonzero components of (g_α). Note that $n \geqslant 1$ because otherwise $0 \neq g_0 = \sum_{\alpha\in A} g_\alpha = 0$, a contradiction. Then

$$g_{\alpha_0} = -\textstyle\sum_{i=1}^n g_{\alpha_i} \in G_{\alpha_0} \cap \sum_{i=1}^n G_{\alpha_i} = \{0\}$$

and so $g_0 = 0$, a contradiction. Thus, $(g_\alpha) = (0)$ and so φ is injective. □

DEFINITION 18.3. Given any set A and any abelian group G, set $G^{(A)} = \oplus_{\alpha\in A} G$ the direct sum of A many copies of G. An abelian group G is *free* if there exists a set A such that $G \cong \mathbb{Z}^{(A)} = \oplus_{\alpha\in A}\mathbb{Z}$. In $\mathbb{Z}^{(A)}$, for each $\beta \in A$, let $\mathbf{e}_\beta = (\delta_{\alpha\beta})$ where

$$\delta_{\alpha\beta} = \begin{cases} 1 & \text{if } \alpha = \beta \\ 0 & \text{if } \alpha \neq \beta. \end{cases}$$

That is, $\mathbf{e}_\beta$ is the sequence with 1 in the β spot and 0 everywhere else.

Be warned that a free group is not usually the same as a free abelian group.

DEFINITION 18.4. Let G be an abelian group. A *basis* for G is a subset $B \subseteq G$ such that, for all $0 \neq g \in G$ there exist unique $m \in \mathbb{N}$, distinct $b_1, \dots, b_m \in B$, and $n_{b_1}, \dots, n_{b_m} \in \mathbb{Z} - \{0\}$ such that $g = \sum_{i=1}^m n_{b_i} b_i$. We sometimes write $\sum_b^{\text{finite}} n_b b$ in place of $\sum_{i=1}^m n_{b_i} b_i$.

EXAMPLE 18.5. Let A be a set. The set $\{\mathbf{e}_\beta \mid \beta \in A\}$ is a basis for $\mathbb{Z}^{(A)}$.

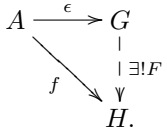
Be warned that not every abelian group has a basis.

EXAMPLE 18.6. If n is an integer $n \geqslant 2$, then $\mathbb{Z}/n\mathbb{Z}$ does not have a basis. Indeed, for each element $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$, we have $n\overline{m} = 0$ and so no subset of $\mathbb{Z}/n\mathbb{Z}$ is linearly independent over $\mathbb{Z}$.

The next proposition contains the universal property for free abelian groups and the fact that the universal property characterizes free abelian groups up to isomorphism.

PROPOSITION 18.7. *For an abelian group G and a function $\epsilon\colon A \hookrightarrow G$, TFAE:*

(i) *there is an isomorphism $\varphi\colon \mathbb{Z}^{(A)} \to G$ such that $\varphi(\mathbf{e}_\alpha) = \epsilon(\alpha)$ for each $\alpha \in A$;*
(ii) *$\epsilon(A)$ is a basis for G;*
(iii) *for each abelian group H and each function $f\colon A \to H$, there is a unique abelian group homomorphism $F\colon G \to H$ making the following diagram commute:*



PROOF. (i) $\implies$ (ii). Let $\varphi\colon \mathbb{Z}^{(A)} \to G$ be such an isomorphism. The set $\{\mathbf{e}_\alpha \mid \alpha \in A\} \subseteq \mathbb{Z}^{(A)}$ is a basis for $\mathbb{Z}^{(A)}$. Because φ is an isomorphism, the set

$$\epsilon(A) = \varphi(\{\mathbf{e}_\alpha \mid \alpha \in A\}) \subseteq G$$

is a basis for G.

(ii) $\implies$ (iii). Define $F\colon G \to H$ by the formula

$$F\left(\sum_\alpha^{\text{finite}} n_\alpha \epsilon(\alpha)\right) = \sum_\alpha^{\text{finite}} n_\alpha f(\alpha).$$

The fact that $\epsilon(A)$ is a basis for G shows that F is a well-defined abelian group homomorphism. The next computation shows that the diagram commutes: for $\beta \in A$, we have

$$F(\epsilon(\beta)) = F\left(\textstyle\sum_\alpha \delta_{\alpha\beta}\epsilon(\alpha)\right) = \sum_\alpha \delta_{\alpha\beta} f(\alpha) = f(\beta).$$

For the uniqueness, assume that $F'\colon G \to H$ is another homomorphism such that $F'(\epsilon(\beta)) = f(\beta)$ for all $\beta \in A$. Then

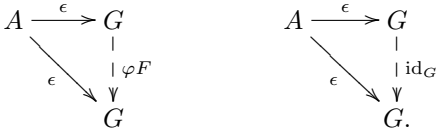
$$F'\left(\sum_\alpha^{\text{finite}} n_\alpha \epsilon(\alpha)\right) = \sum_\alpha^{\text{finite}} n_\alpha F'(\epsilon(\alpha)) = \sum_\alpha^{\text{finite}} n_\alpha f(\alpha) = F\left(\sum_\alpha^{\text{finite}} n_\alpha \epsilon(\alpha)\right)$$

(iii) $\implies$ (i). Let $f\colon A \to \mathbb{Z}^{(A)}$ be given by $f(\alpha) = \mathbf{e}_\alpha$. Condition (iii) yields an abelian group homomorphism $F\colon G \to \mathbb{Z}^{(A)}$ such that $F(\epsilon(\beta)) = f(\beta) = \mathbf{e}_\beta$ for all $\beta \in A$. Hence, $F\left(\sum_\alpha^{\text{finite}} n_\alpha \epsilon(\alpha)\right) = \sum_\alpha^{\text{finite}} n_\alpha \mathbf{e}_\alpha$. Because $\mathbb{Z}^{(A)}$ has a basis $\{\mathbf{e}_\alpha\}_{\alpha\in A}$, the implication (ii) $\implies$ (iii) shows that there exists a unique abelian group homomorphism $\varphi\colon \mathbb{Z}^{(A)} \to G$ such that $\varphi(\mathbf{e}_\alpha) = \epsilon(\alpha)$ for each $\alpha \in A$.

It follows that $\varphi F = \mathrm{id}_G$ because of the uniqueness condition in (iii): The map $\varphi F\colon G \to G$ satisfies

$$(\varphi F)(\epsilon(\alpha)) = \varphi(F(\epsilon(\alpha))) = \varphi(\mathbf{e}_\alpha) = \epsilon(\alpha).$$

In other words, the following diagrams commute:



Since there is a unique abelian group homomorphism making the diagram commute, we have $\varphi F = \mathrm{id}_G$. Similarly, applying condition (iii) to $\mathbb{Z}^{(A)}$, the uniqueness statement shows $F\varphi = \mathrm{id}_{\mathbb{Z}^{(A)}}$ and so F and φ are inverse isomorphisms. □

19. Day 21

Here is a restatement of the universal property for clarification.

COROLLARY 19.1. *Let G be a free abelian group, and let $B \subseteq G$ be a basis for G. For every abelian group H and every subset $\{h_b\}_{b\in B} \subseteq H$, there exists a unique abelian group homomorphism $F\colon G \to H$ such that, for each $b \in B$, we have $F(b) = h_b$.* □

DEFINITION 19.2. Let G be an abelian group. G is *torsion* if, for each $g \in G$ there exists $n \in \mathbb{N}$ such that $ng = 0$. G is *torsion-free* if, for each $0 \neq g \in G$ the map $\mathbb{N} \to G$ given by $n \mapsto ng$ is injective.

Note that there are groups that are not torsion and not torsion-free: $\mathbb{Z}\oplus(\mathbb{Z}/2\mathbb{Z})$.

THEOREM 19.3. *Let G be a torsion group. For each prime number p, set $G_p = \{g \in G \mid p^n g = 0 \text{ for some } n \in \mathbb{N}\}$. Then each $G_p \leqslant G$ and $G \cong \oplus_p G_p$.*

PROOF. First we show $G_p \leqslant G$. Because $p^j 0 = 0$ for all $j \in \mathbb{N}$, we have $0 \in G_p$. Fix $g, h \in G_p$ and let $m, n \in \mathbb{N}$ such that $p^m g = 0 = p^n h$. With $r = \max\{m, n\}$, we have $p^r g = 0 = p^r h$. Hence, $p^r(g - h) = p^r g - p^r h = 0$ and so $g - h \in G_p$. Now apply the subgroup test.

Next we show $G \cong \oplus_p G_p$. We will use Proposition 18.2, so there are two things to check.

(1) $G = \sum_p G_p$. Fix $g \in G$. Because G is torsion, there exists $n \geqslant 2$ such that $ng = 0$. Write $n = p^r m$ where $p \nmid m$. Then $\gcd(p^r, m) = 1$ and so there are integers $a, b \in \mathbb{Z}$ such that $ap^r + bm = 1$. It follows that $ap^r g + bmg = g$ and $m(ap^r g) = 0 = p^r(bmg)$. That is, we can write $g = g_p + g'$ where $g_p \in G_p$ and $mg' = 0$.

Using the Fundamental Theorem of Arithmetic, write $n = p_1^{r_1} \cdots p_m^{r_m}$ where the p_i are distinct primes. By induction on m, using the previous paragraph, we can write $g = g_{p_1} + \ldots + g_{p_m}$ for some $g_{p_i} \in G_{p_i}$. This shows $G = \sum_p G_p$.

(2) For all $n \in \mathbb{N}$ and all distinct prime numbers $p_0, p_1, \ldots, p_n$ we have $G_{p_0} \cap \sum_{i=1}^n G_{p_i} = \{0\}$. Suppose $g_0 \in G_{p_0} \cap \sum_{i=1}^n G_{p_i}$, say $g_0 = \sum_{i=1}^n g_i$ with $g_i \in G_{p_i}$. For each $i = 0, \ldots, n$ there exists $a_i \geqslant 1$ such that $p_i^{a_i} g_i = 0$. Let $m = p_1^{a_1} \cdots p_n^{a_n}$ and note that $\gcd(p_0^{a_0}, m) = 1$. Hence, there are integers $c, d \in \mathbb{Z}$ such that $cp_0^{a_0} + dm = 1$. By construction and assumption, we have

$$mg_0 = m \textstyle\sum_{i=1}^n g_i = 0 = p_0^{a_0} g_0$$

and so

$$g_0 = 1g_0 = (cp_0^{a_0} + dm)g_0 = cp_0^{a_0} g_0 + dmg_0 = 0$$

as desired. □

COROLLARY 19.4. *If G is a finite abelian group, then $G \cong G_{p_1} \oplus \cdots \oplus G_{p_n}$ where $p_1, \ldots, p_n$ are the distinct prime factors of $|G|$.*

PROOF. G is finite, so every element of G has finite order. Hence, G is torsion and so $G \cong \oplus_p G_p$. If $p \nmid |G|$, then $G_p = \{0\}$: otherwise, there exists an element $0 \neq g \in G_p$ and so $p \big| |g| \big| |G|$, a contradiction. □

Here's something important that does not follow from the "usual" axioms of set theory. See Hungerford pp. 12-15 for a discussion.

The Axiom of Choice. *The Cartesian product of a family of nonempty sets indexed over a nonempty set is nonempty.*

For an important reformulation, we need some terminology.

DEFINITION 19.5. A *partially ordered set* is a nonempty set A with a relation $\leqslant$ (called a *partial ordering on A*) which is reflexive (for all $a \in A$, we have $a \leqslant a$), transitive (for all $a, b, c \in A$, if $a \leqslant b$ and $b \leqslant c$, then $a \leqslant c$) and antisymmetric (for all $a, b \in A$, if $a \leqslant b$ and $b \leqslant a$, then $a = b$).

EXAMPLE 19.6. If $A \subseteq \mathbb{R}$, then A is a partially ordered set under the usually ordering $\leqslant$.

If S is a set and A is a set of subsets of S, then A is a partially ordered set under inclusion.

DEFINITION 19.7. Assume that A is a partially ordered set. Two elements $a, b \in A$ are *comparable* if either $a \leqslant b$ or $b \leqslant a$. An element $c \in A$ is *maximal* in A if, for every $a \in A$ which is comparable to c, we have $a \leqslant c$. If $\emptyset \neq B \subseteq A$, then an *upper bound* of B in A is an element $a \in A$ such that, for all $b \in B$, we have $b \leqslant a$. B is a *chain* if every two elements in B are comparable.

Assuming the "usual" axioms of set theory, the following is equivalent to the Axiom of Choice. For a proof, consult a book on set theory.

Zorn's Lemma *Let A be a nonempty partially ordered set such that every chain in A has an upper bound in A. Then A contains a maximal element.*

Here is a useful application of Zorn's Lemma.

LEMMA 19.8. *Let G be an abelian group and $G' \leqslant G$. The set $\mathcal{H} = \{H \leqslant G \mid G' \cap H = \{0\}\}$ has a maximal element.*

PROOF. First, we have $\{0\} \in \mathcal{H}$, and so $\mathcal{H} \neq \emptyset$. The set $\mathcal{H}$ is partially ordered with respect to inclusion, so it suffices to show that every chain $\mathcal{C}$ in $\mathcal{H}$ has an upper bound in $\mathcal{H}$.

We claim that $K = \cup_{H \in \mathcal{C}} H$ is an upper bound for $\mathcal{C}$ in $\mathcal{H}$. (Then the result will follow from Zorn's Lemma.) There are three things to check:

(1) $K \leqslant G$: We use the subgroup test. $\mathcal{C}$ is a chain, so it is nonempty. For each $H \in \mathcal{C}$, we have $H \leqslant G$ and so $0 \in H \subseteq K$ implies $0 \in K$. Let $h, h' \in K$. We need to show $h - h' \in K$. By definition, there exist $H, H' \in \mathcal{C}$ such that $h \in H$ and $h' \in H'$. Since $\mathcal{C}$ is a chain, either $H \subseteq H'$ or $H' \subseteq H$. Assume that $H \subseteq H'$. (The other case is similar.) Then $h \in H \subseteq H'$ and $h' \in H'$ and so $h - h' \in H' \subseteq K$.

(2) $G' \cap K = \{0\}$: $G' \cap K = G' \cap (\cup_{H \in \mathcal{C}} H) = \cup_{H \in \mathcal{C}} (G' \cap H) = \cup_{H \in \mathcal{C}} \{0\} = \{0\}$.

(3) For all $H' \in \mathcal{C}$, we have $H' \subseteq K$. This is true by the definition: $H' \in \mathcal{C}$ implies $H' \subseteq \cup_{H \in \mathcal{C}} H = K$. □

20. Day 22

THEOREM 20.1. *Let G be an abelian group. Assume that p is a prime number such that $p^n G = \{0\}$ and $p^{n-1} G \neq \{0\}$ for some $n \geqslant 1$. Then there exists $H \leqslant G$ such that $G \cong \mathbb{Z}/p^n\mathbb{Z} \oplus H$.*

PROOF. By the choice of p and n, there exists $0 \neq g \in G$ such that $|g| = p^n$. Hence $\langle g \rangle \cong \mathbb{Z}/p^n\mathbb{Z}$ and so it suffices to find $H \leqslant G$ such that $G \cong \langle g \rangle \oplus H$. By Proposition 18.2 it suffices to find $H \leqslant G$ such that $G = \langle g \rangle + H$ and $\langle g \rangle \cap H = \{0\}$.

Lemma 19.8 implies that the set $\mathcal{H} = \{H \leqslant G \mid \langle g \rangle \cap H = \{0\}\}$ contains a maximal element H with respect to inclusion. By construction, we have $\langle g \rangle \cap H = \{0\}$.

Suppose $G \supsetneq \langle g \rangle + H$, and fix $k \in G - (\langle g \rangle + H)$.

Suppose $pk \in \langle g \rangle + H$. Then we have $pk = rg + h$ for some $r \in \mathbb{Z}$ and $h \in H$. Then

$$0 = p^n k = p^{n-1}(pk) = p^{n-1} rg + p^{n-1} h$$

and so

$$p^{n-1} rg = -p^{n-1} h \in \langle g \rangle \cap H = \{0\}$$

and so $p^{n-1}rg = 0$. Since $|g| = p^n$, it follows that $p \big| r$. Write $r = ps$ for some $s \in \mathbb{Z}$. Then

$$pk = rg + h = psg + h.$$

Let $k' = k - sg$. Then $k' \notin \langle g \rangle + H$: otherwise $k', sg \in \langle g \rangle + H$ implies $k = k' + sg \in \langle g \rangle + H$, a contradiction. Also,

$$pk' = pk - psg = pk - rg = h \in H.$$

Claim: $(\langle k' \rangle + H) \cap \langle g \rangle = \{0\}$.

An element of $(\langle k' \rangle + H) \cap \langle g \rangle$ has the form $tk' + h' = ug$ with $h' \in H$ and $t, u \in \mathbb{Z}$. We need to show $ug = 0$. We have

$$tk' = ug - h' \in \langle g \rangle + H.$$

Also,

$$tk' = tk - tsg \implies tk = tk' + tsg \in \langle g \rangle + H$$

and so $p \big| t$; say $t = pv$ with $v \in \mathbb{Z}$. Then

$$ug = h' + tk' = h' + pvk' = h' + vh \in H.$$

Since $ug \in \langle g \rangle$ we have $ug \in \langle g \rangle \cap H = \{0\}$ and so $ug = 0$.

Since $k' \notin H$, we have $H \subsetneq \langle k' \rangle + H$, so the claim violates the maximality of H. Thus, $pk \notin \langle g \rangle + H$. Since $p^n G = 0$, there exists $m \in \mathbb{N}$ such that $p^m k \in \langle g \rangle + H$ and $p^{m-1}k \notin \langle g \rangle + H$. That is, $z = p^{m-1}k$ is an element of G such that $z \notin \langle g \rangle + H$ and $pz \in \langle g \rangle + H$. Thus, the above argument again yields a contradiction, and so the element k cannot exist. □

Proposition 20.2. *Every subgroup of $\mathbb{Z}^n$ is free of rank $\leqslant n$.*

Proof. By induction on n. If $n = 1$, then every subgroup $H \leqslant \mathbb{Z}$ is $H = m\mathbb{Z}$ for some $m \in \mathbb{Z}$. Therefore,

$$H = \begin{cases} \{0\} \cong \mathbb{Z}^0 & \text{if } m = 0 \\ m\mathbb{Z} \cong \mathbb{Z}^1 & \text{if } m \neq 0. \end{cases}$$

Assume $n > 1$ and assume that every subgroup of $\mathbb{Z}^{n-1}$ is free of rank $\leqslant n-1$. Let $K \leqslant \mathbb{Z}^n$, and define $f \colon \mathbb{Z}^n \to \mathbb{Z}$ by the formula $f(a_1, \ldots, a_n) = a_n$. Check that f is a homomorphism with $\mathrm{Ker}(f) = \mathbb{Z}^{n-1} \oplus \{0\} \cong \mathbb{Z}^{n-1}$. It follows that $f(K) \leqslant \mathbb{Z}$, so $f(K) = m\mathbb{Z}$ for some $m \in \mathbb{Z}$. If $m = 0$, then $K \subseteq \mathrm{Ker}(f) = \mathbb{Z}^{n-1}$, so our induction hypothesis implies that K is free of rank $\leqslant n-1$. So, we assume that $m \neq 0$. Fix an element $k \in K$ such that $f(k) = m$.

Claim: $K = (K \cap \mathbb{Z}^{n-1}) + \langle k \rangle$. The containment "$\supseteq$" is clear. For the containment "$\subseteq$" fix an element $h \in K$. Then $f(h) = rm$ for some $r \in \mathbb{Z}$, so $f(h - rk) = 0$. Hence, we have $h - rk \in \mathrm{Ker}(f) \cap K = \mathbb{Z}^{n-1} \cap K$, and so $h \in (K \cap \mathbb{Z}^{n-1}) + \langle k \rangle$.

Claim: $(K \cap \mathbb{Z}^{n-1}) \cap \langle k \rangle = \{0\}$. Write $k = (k_1, \ldots, k_n)$, and let

$$h = (h_1, \ldots, h_{n-1}, 0) \in (K \cap \mathbb{Z}^{n-1}) \cap \langle k \rangle.$$

Since $h \in \langle k \rangle$, we have

$$(h_1, \ldots, h_{n-1}, 0) = h = sk = (sk_1, \ldots, sk_n)$$

for some $s \in \mathbb{Z}$, and so $0 = sk_n = sm$. Since $m \neq 0$, we have $s = 0$ and so $h = sk = 0$.

Using the two claims, Proposition 18.2 implies $K \cong (K \cap \mathbb{Z}^{n-1}) \oplus \langle k \rangle$. Since $K \cap \mathbb{Z}^{n-1} \leqslant \mathbb{Z}^{n-1}$, we have $K \cap \mathbb{Z}^{n-1} \cong \mathbb{Z}^{k-1}$ for some $k-1 \leqslant n-1$. Also, since $k \neq 0$, we have $\langle k \rangle \cong \mathbb{Z}$ and so

$$K \cong (K \cap \mathbb{Z}^{n-1}) \oplus \langle k \rangle \cong \mathbb{Z}^{k-1} \oplus \mathbb{Z}^1 \cong \mathbb{Z}^k$$

as desired. □

21. Day 23

REMARK 21.1. Fix integers $n, k \geqslant 1$ and let $h\colon \mathbb{Z}^k \to \mathbb{Z}^n$ be a group homomorphism. We can represent h by an $n \times k$ matrix with entries in $\mathbb{Z}$ as follows. Write elements of $\mathbb{Z}^k$ and $\mathbb{Z}^n$ as column vectors with entries in $\mathbb{Z}$. Let $\mathbf{e}_1, \dots, \mathbf{e}_k \in \mathbb{Z}^k$ be the standard basis. For $j = 1, \dots, k$ write

$$h(\mathbf{e}_j) = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{i,j} \\ \vdots \\ a_{n,j} \end{pmatrix}.$$

Then h is represented by the $n \times k$ matrix

$$[f] = (a_{i,j}) = \begin{pmatrix} a_{1,1} & \cdots & a_{1,j} & \cdots & a_{1,k} \\ \vdots & & \vdots & & \vdots \\ a_{i,1} & \cdots & a_{i,j} & \cdots & a_{i,k} \\ \vdots & & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,j} & \cdots & a_{n,k} \end{pmatrix}$$

in the following sense: For each vector

$$\begin{pmatrix} r_1 \\ \vdots \\ r_k \end{pmatrix} \in \mathbb{Z}^k$$

we have

$$h\begin{pmatrix} r_1 \\ \vdots \\ r_k \end{pmatrix} = h(\textstyle\sum_j r_j \mathbf{e}_j) = \sum_j r_j h(\mathbf{e}_j) = \sum_j r_j \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{n,j} \end{pmatrix} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,k} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,k} \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_k \end{pmatrix}.$$

We have elementary basis operations on the $\mathbf{e}_j$:

(1) Replace $\mathbf{e}_j$ with $-\mathbf{e}_j$;
(2) Interchange $\mathbf{e}_j$ and $\mathbf{e}_l$;
(3) Replace $\mathbf{e}_j$ with $\mathbf{e}_j + r\mathbf{e}_l$ for some $r \in \mathbb{Z}$ and $l \neq j$.

These correspond to the appropriate elementary column operations on the matrix $(a_{i,j})$, in the following sense. Applying one of the elementary basis operations to the $\mathbf{e}_j$ yields an isomorphism $\Phi\colon \mathbb{Z}^k \to \mathbb{Z}^k$ such that the following diagram commutes

$$\begin{array}{ccc} \mathbb{Z}^k & \xrightarrow{(a_{i,j})} & \mathbb{Z}^n \\ {\scriptstyle\Phi}\downarrow{\scriptstyle\cong} & & \downarrow{\scriptstyle=} \\ \mathbb{Z}^k & \xrightarrow{(b_{i,j})} & \mathbb{Z}^n \end{array}$$

where $(b_{i,j})$ is the matrix obtained by applying the corresponding elementary column operation to the matrix $(a_{i,j})$. And, conversely, if $(b_{i,j})$ is obtained from $(a_{i,j})$ by an elementary column operation, then the corresponding elementary basis operations on the $\mathbf{e}_j$ yields a commutative diagram as above.

Let $\mathbf{f}_1, \dots, \mathbf{f}_n \in \mathbb{Z}^n$ be the standard basis. The elementary basis operations on the $\mathbf{f}_j$ correspond similarly to the elementary row operations on the matrix $(a_{i,j})$.

Furthermore, if we repeatedly apply elementary row and column operations to the matrix $(a_{i,j})$ to obtain the matrix $(c_{i,j})$, then this yields a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}^k & \xrightarrow{(a_{i,j})} & \mathbb{Z}^n \\ {\scriptstyle\Phi}\downarrow\cong & & {\scriptstyle\Psi}\downarrow\cong \\ \mathbb{Z}^k & \xrightarrow{(c_{i,j})} & \mathbb{Z}^n. \end{array}$$

We say that an $n \times k$ matrix $(d_{i,j})$ with integer entries is *equivalent* to $(a_{i,j})$ if it can be obtained from $(a_{i,j})$ using a (finite) sequence of elementary row and column operations.

PROPOSITION 21.2. *Fix integers $n \geqslant k \geqslant 1$ and let $h\colon \mathbb{Z}^k \to \mathbb{Z}^n$ be a group monomorphism. There exists a commutative diagram of group homomorphisms*

$$\begin{array}{ccc} \mathbb{Z}^k & \xrightarrow{h} & \mathbb{Z}^n \\ {\scriptstyle\Phi}\downarrow\cong & & {\scriptstyle\Psi}\downarrow\cong \\ \mathbb{Z}^k & \xrightarrow{h'} & \mathbb{Z}^n \end{array}$$

such that the matrix representing h' is "diagonal", that is, $[h'] = (d_{i,j})$ where $d_{i,j} = 0$ when $i \neq j$. Furthermore, $(d_{i,j})$ may be constructed so that $d_{1,1} \big| d_{2,2} \big| \cdots \big| d_{k,k}$.

PROOF. Let $[h] = (a_{i,j})$, and let A denote the set of all $s \in \mathbb{N}$ such that a finite number of elementary row and column operations applied to $(a_{i,j})$ yields a matrix with s in the upper left corner.

Claim: $A \neq \emptyset$. Because h is a monomorphism, there is a nonzero entry in the first column of $(a_{i,j})$. Hence, matrix operations can be applied to yield a matrix with a positive entry in the first column, and then to yield a matrix with a positive entry in the $1,1$ entry.

Because A is a nonempty set of natural numbers, it has a minimal element. Apply the necessary row and column operations to yield a new matrix $(b_{i,j})$ such that $b_{1,1}$ is the smallest element of A.

Claim: $b_{1,1} \leqslant |b_{i,j}|$ for all $b_{i,j} \neq 0$. Suppose not, say $0 < |b_{i,j}| < b_{1,1}$. Elementary matrix operations would then yield an equivalent matrix with $|b_{i,j}|$ in the i,j spot, and then an equivalent matrix with $|b_{i,j}|$ in the $1,1$ spot. This contradicts the minimality of $b_{1,1}$ in A.

Claim: $b_{1,1} \big| b_{i,j}$ for all i,j. Use the division algorithm to find integers q, r such that $b_{i,j} = qb_{1,1} + r$ and $0 \leqslant r < b_{1,1}$. If $r \neq 0$, then elementary matrix operations can be applied to yield an equivalent matrix with r in the $1,1$ spot; this would contradict the minimality of $b_{1,1}$ in A. Hence, $r = 0$ and so $b_{1,1} \big| b_{i,j}$.

It follows that elementary matrix operations yield an equivalent matrix $(c_{i,j})$ such that $r \neq 1$ implies $c_{1,r} = 0$ and $c_{r,1} = 0$ and such that $c_{1,1} \big| c_{i,j}$ for each i,j.

Repeating this process to appropriate "submatrices" of $(c_{i,j})$ yields the desired matrix, and Remark 21.1 yields the desired commutative diagram. □

PROPOSITION 21.3. *Let $h\colon K \to N$ and $h'\colon K' \to N'$ be abelian group homomorphisms. Given a commutative diagram of group homomorphisms*

$$\begin{array}{ccc} K & \xrightarrow{h} & N \\ {\scriptstyle\Phi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\Psi}\downarrow{\scriptstyle\cong} \\ K' & \xrightarrow{h'} & N' \end{array}$$

there is an isomorphism $\alpha\colon N/\operatorname{Im}(h) \xrightarrow{\cong} N'/\operatorname{Im}(h')$.

PROOF. Let $\alpha\colon N/\operatorname{Im}(h) \to N'/\operatorname{Im}(h')$ be given by

$$\alpha(x + \operatorname{Im}(h)) = \Psi(x) + \operatorname{Im}(h').$$

Claim: α is well-defined. Fix $x, y \in N$ such that $x + \operatorname{Im}(h) = y + \operatorname{Im}(h)$. Then $x - y \in \operatorname{Im}(h)$, say $x - y = h(z)$ with $z \in K$. Then

$$\Psi(x) - \Psi(y) = \Psi(x - y) = \Psi(h(z)) = h'(\Phi(z)) \in \operatorname{Im}(h')$$

and so $\Psi(x) + \operatorname{Im}(h') = \Psi(y) + \operatorname{Im}(h')$.

Since Ψ is a group homomorphism, one checks readily that α is also a group homomorphism. (The fact that α is a well-defined group homomorphism can also be shown using the universal property for group quotients in Lemma 9.2.)

Since Ψ and Φ are isomorphism, we have a second commutative diagram of abelian group homomorphisms

$$\begin{array}{ccc} K' & \xrightarrow{h'} & N' \\ {\scriptstyle\Phi^{-1}}\downarrow{\scriptstyle\cong} & & {\scriptstyle\Psi^{-1}}\downarrow{\scriptstyle\cong} \\ K & \xrightarrow{h} & N \end{array}$$

Indeed, for $k' \in K'$ we have

$$\Psi(h(\Phi^{-1}(k'))) = h'(\Phi(\Phi^{-1}(k'))) = h'(k') = \Psi(\Psi^{-1}(h'(k')))$$

and so $h(\Phi^{-1}(k')) = \Psi^{-1}(h'(k'))$.

Thus, the above argument shows that the map $\beta\colon N'/\operatorname{Im}(h') \to N/\operatorname{Im}(h)$ given by $\beta(x' + \operatorname{Im}(h')) = \Psi^{-1}(x') + \operatorname{Im}(h)$ is a well-defined abelian group homomorphism. Direct computation shows $\beta\alpha = \mathrm{id}_{N/\operatorname{Im}(h)}$ and $\alpha\beta = \mathrm{id}_{N'/\operatorname{Im}(h')}$. Hence, α is an isomorphism with inverse β. □

22. Day 24

Here is the Fundamental Theorem for Finitely Generated Abelian Groups.

THEOREM 22.1. *If G is a finitely generated abelian group, then G is a direct sum of cyclic groups. Moreover, there is an isomorphism*

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}^{n-k}$$

such that each $d_i \geqslant 1$ and $d_1 \big| d_2 \big| \cdots \big| d_k$.

PROOF. Let $\{g_1, \ldots, g_n\} \subseteq G$ be a generating set for G. The map $f\colon \mathbb{Z}^n \to G$ given by $f(m_1, \ldots, m_n) = \sum_i m_i g_i$ is a well-defined group epimorphism. We have $\operatorname{Ker}(f) \leqslant \mathbb{Z}^n$, so Proposition 20.2 yields an isomorphism $h_1\colon \mathbb{Z}^k \xrightarrow{\cong} \operatorname{Ker}(f)$ for some $k \leqslant n$. Let $\varepsilon\colon \operatorname{Ker}(f) \to \mathbb{Z}^n$ be the natural inclusion, and set $h = \varepsilon h_1\colon \mathbb{Z}^k \to$

$\mathbb{Z}^n$. Since h_1 is an isomorphism and ε is a monomorphism, we know that h is a monomorphism.

Proposition 21.2 yields a commutative diagram of group homomorphisms

$$\begin{array}{ccc} \mathbb{Z}^k & \xrightarrow{h} & \mathbb{Z}^n \\ {\scriptstyle\Phi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\Psi}\downarrow{\scriptstyle\cong} \\ \mathbb{Z}^k & \xrightarrow{h'} & \mathbb{Z}^n \end{array}$$

such that $[h'] = (d_{i,j})$ where $d_{i,j} = 0$ when $i \neq j$ and $d_{1,1}\big|d_{2,2}\big|\cdots\big|d_{k,k}$. Let $\mathbf{f}_1, \ldots, \mathbf{f}_n \in \mathbb{Z}^n$ be the standard basis. Then we have

$$\begin{aligned} G &\cong \mathbb{Z}^n/\operatorname{Ker}(f) && \text{first isomorphism theorem} \\ &= \mathbb{Z}^n/\operatorname{Im}(h) && \text{construction of } h \\ &\cong \mathbb{Z}^n/\operatorname{Im}(h') && \text{Proposition 21.3} \\ &= \mathbb{Z}^n/\langle d_{1,1}\mathbf{f}_1, \ldots, d_{k,k}\mathbf{f}_k\rangle && \text{assumptions on } h' \\ &\cong \mathbb{Z}/d_{1,1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_{k,k}\mathbb{Z} \oplus \mathbb{Z}^{n-k} && \text{Exercise.} \end{aligned}$$

This is the desired conclusion. □

Corollary 22.2. *Let G be a finitely generated abelian group and set $G_{tor} = \{g \in G \mid ng = 0 \text{ for some } n \in \mathbb{Z}\}$. If G is generated by n elements, then there exists an integer $0 \leqslant l \leqslant n$ such that $G \cong G_{tor} \oplus \mathbb{Z}^l$.*

Proof. Using Theorem 22.1 we have

$$\varphi\colon \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}^{n-k} \xrightarrow{\cong} G$$

such that each $d_i \geqslant 1$ and $d_1\big|d_2\big|\cdots\big|d_k$.

Note that $(\overline{g_1}, \ldots, \overline{g_k}, g_{k+1}, \ldots, g_n) \in (\oplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}) \oplus \mathbb{Z}^{n-k}$ is a torsion element if and only if $g_{k+1} = \cdots = g_n = 0$. That is, we have

$$((\oplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}) \oplus \mathbb{Z}^{n-k})_{\text{tor}} = (\oplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}) \oplus \{0\}$$

Since φ is an isomorphism, we have

$$G_{\text{tor}} = \varphi(((\oplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}) \oplus \mathbb{Z}^{n-k})_{\text{tor}}) = \varphi((\oplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}) \oplus \{0\})$$

and so

$$G = \varphi((\oplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}) \oplus \mathbb{Z}^{n-k}) \cong \varphi(\oplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}) \oplus \varphi(\mathbb{Z}^{n-k}) \cong G_{\text{tor}} \oplus \mathbb{Z}^{n-k}$$

as desired. □

Given a finitely generated abelian group, there are several ways to write G_{tor}. Each one has its own utility. Since G_{tor} is finite (exercise) the final results from this chapter show some of the ways.

Proposition 22.3. *Let G be a finite abelian group. If p is a prime number such that $p^n G = \{0\}$ for some $n \geqslant 1$, then there exist $n_1, \ldots, n_r \in \mathbb{N}$ such that $G \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_r}\mathbb{Z}$.*

Proof. By induction on $|G|$, using Theorem 20.1. □

Corollary 22.4. *Let G be a finite abelian group and $p_1, \ldots, p_s$ the distinct prime divisors of $|G|$. There are $n_{1,1}, \ldots, n_{1,r_1}, n_{2,1}, \ldots, n_{2,r_2}, \ldots, n_{s,1}, \ldots, n_{s,r_s} \in \mathbb{N}$ such that $G \cong \oplus_{i=1}^s \oplus_{j=1}^{n_{j,r_j}} \mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}$.*

PROOF. By Theorems 19.3 and Proposition 22.3. □

COROLLARY 22.5. *If G is a finite abelian group, then there are $d_1, \dots, d_k \in \mathbb{N}$ such that*

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z}$$

and $d_1 \big| d_2 \big| \cdots \big| d_k$.

PROOF. By Theorem 22.1, using the fact that a finite group cannot have an infinite direct summand. □

CHAPTER 2

Category Theory

1. Day 1

DEFINITION 1.1. A *category* $\mathcal{C}$ is a collection (or class) $\mathrm{Ob}(\mathcal{C})$ of "objects" such that, for every pair A, B in $\mathrm{Ob}(\mathcal{C})$ there is an associated set $\mathrm{Mor}_{\mathcal{C}}(A, B)$ of "morphisms" satisfying the following properties:

(1) If A, B, C, D are in $\mathrm{Ob}(\mathcal{C})$, and either $A \neq C$ or $B \neq D$, then $\mathrm{Mor}_{\mathcal{C}}(A, B)$ and $\mathrm{Mor}_{\mathcal{C}}(C, D)$ are disjoint;
(2) If A, B, C are in $\mathrm{Ob}(\mathcal{C})$, there is a map $\mathrm{Mor}_{\mathcal{C}}(B, C) \times \mathrm{Mor}_{\mathcal{C}}(A, B) \to \mathrm{Mor}_{\mathcal{C}}(A, C)$, called a *law of composition* and denoted $(f, g) \mapsto f \circ g$;
(3) The law of composition is associative; and
(4) For each A in $\mathrm{Ob}(\mathcal{C})$, there is an element $i_A \in \mathrm{Mor}_{\mathcal{C}}(A, A)$ such that for all $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$ and $g \in \mathrm{Mor}_{\mathcal{C}}(C, A)$ we have $f \circ i_A = f$ and $i_A \circ g = g$.

Instead of writing $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$, we often write "$f\colon A \to B$ is a morphism in $\mathcal{C}$".

EXAMPLE 1.2. The category of sets: $\underline{\text{sets}}$ is the category whose collection of objects is exactly the collection of all sets and such that, for sets A, B the set $\mathrm{Mor}_{\underline{\text{sets}}}(A, B)$ is the set of all functions $f\colon A \to B$. We set $i_A = \mathrm{id}_A\colon A \to A$ and $f \circ g$ is the composition of functions.

EXAMPLE 1.3. The category of groups: $\underline{\text{gps}}$ is the category whose collection of objects is exactly the collection of all groups and such that, for groups A, B the set $\mathrm{Mor}_{\underline{\text{gps}}}(A, B)$ is the set of all group homomorphisms $f\colon A \to B$. We set $i_A = \mathrm{id}_A\colon A \to A$ and $f \circ g$ is the composition of functions. Note that, in verifying that $\underline{\text{gps}}$ is a category, we use the fact that the composition of two group homomorphisms is another group homomorphism.

EXAMPLE 1.4. The category of abelian groups: $\underline{\text{ab}}$ is the category whose collection of objects is exactly the collection of all abelian groups and such that, for abelian groups A, B the set $\mathrm{Mor}_{\underline{\text{ab}}}(A, B)$ is the set of all (abelian) group homomorphisms $f\colon A \to B$. We set $i_A = \mathrm{id}_A\colon A \to A$ and $f \circ g$ is the composition of functions. (Similarly, we have the categories of finite groups, finitely generated groups, finitely generated abelian groups, finite abelian groups, etc.)

EXAMPLE 1.5. The category of topological spaces: $\underline{\text{top}}$ is the category whose collection of objects is exactly the collection of all topological spaces and such that, for topological spaces A, B the set $\mathrm{Mor}_{\underline{\text{top}}}(A, B)$ is the set of all continuous functions $f\colon A \to B$. We set $i_A = \mathrm{id}_A\colon A \to A$ and $f \circ g$ is the composition of functions. Note that, in verifying that $\underline{\text{top}}$ is a category, we use the fact that the composition of two continuous functions is another continuous function.

EXAMPLE 1.6. The category of complex manifolds: $\underline{\text{man}}$ is the category whose collection of objects is exactly the collection of all complex manifolds and such

that, for complex manifolds A, B the set $\mathrm{Mor}_{\underline{\mathrm{man}}}(A, B)$ is the set of all complex differentiable functions $f\colon A \to B$. We set $i_A = \mathrm{id}_A\colon A \to A$ and $f \circ g$ is the composition of functions. Note that, in verifying that $\underline{\mathrm{top}}$ is a category, we use the fact that the composition of two differentiable functions is differentiable function.

EXAMPLE 1.7. Categories with one object correspond precisely to monoids.

Let M be a monoid. Let $\mathcal{C}$ be the category with $\mathrm{Ob}(\mathcal{C}) = \{M\}$ and $\mathrm{Mor}_{\mathcal{C}}(M, M) = M$. This is a category with one object.

Conversely, let $\mathcal{D}$ be a category with one object A. Then $\mathrm{Mor}_{\mathcal{C}}(A, A)$ is a monoid with multiplication given by the law of composition.

EXAMPLE 1.8. Categories $\mathcal{C}$ such that $\mathrm{Ob}(\mathcal{C})$ is a set and $|\mathrm{Mor}_{\mathcal{C}}(A, B)| \leqslant 1$ for all $A, B \in \mathrm{Ob}(\mathcal{C})$ correspond precisely to partially ordered sets.

Let S be a set partially ordered by $\leqslant$. Let $\mathcal{C}$ be the category such that $\mathrm{Ob}(\mathcal{C}) = S$ and

$$\mathrm{Mor}_{\mathcal{C}}(A, B) = \begin{cases} \{(A, B)\} & \text{if } A \leqslant B \\ \emptyset & \text{if } A \not\leqslant B. \end{cases}$$

Let the law of composition be given by $(A, B) \circ (B, C) = (A, C)$ when $A \leqslant B \leqslant C$.

Conversely, let $\mathcal{D}$ be a category such that $\mathrm{Ob}(\mathcal{D})$ is a set and $|\mathrm{Mor}_{\mathcal{D}}(A, B)| \leqslant 1$ for all $A, B \in \mathrm{Ob}(\mathcal{D})$. We make $\mathrm{Ob}(\mathcal{D})$ into a partially ordered set by declaring $A \leqslant B$ when $\mathrm{Mor}_{\mathcal{D}}(A, B) \neq \emptyset$.

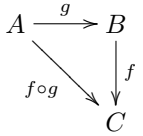
2. Day 2

DEFINITION 2.1. The opposite category: If $\mathcal{C}$ is a category with law of composition $\circ$, define $\mathcal{C}^{\mathrm{op}}$ as $\mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$ and $\mathrm{Mor}_{\mathcal{C}^{\mathrm{op}}}(A, B) = \mathrm{Mor}_{\mathcal{C}}(B, A)$ with law of composition $f * g := g \circ f$. Note that $\mathcal{C}^{\mathrm{op}} = (\mathcal{C}^{\mathrm{op}})^{\mathrm{op}}$.

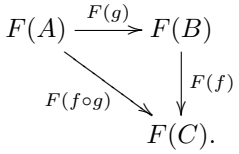
DEFINITION 2.2. Functors: Functors are "maps" between categories that respect the structure of the categories. Let $\mathcal{C}$ and $\mathcal{D}$ be categories.

A *covariant functor* $F\colon \mathcal{C} \to \mathcal{D}$ is a "rule of assignment":

(1) for each object A in $\mathrm{Ob}(\mathcal{C})$, the rule F associates an object $F(A)$ in $\mathrm{Ob}(\mathcal{D})$;
(2) for each morphism $f\colon A \to B$ in $\mathrm{Mor}_{\mathcal{C}}(A, B)$, the rule F associates a morphism $F(f)\colon F(A) \to F(B)$ in $\mathrm{Mor}_{\mathcal{D}}(F(A), F(B))$;
(3) for each object A in $\mathrm{Ob}(\mathcal{C})$, if i_A is the identity morphism in $\mathrm{Mor}_{\mathcal{C}}(A, A)$, then $F(i_A) = i_{F(A)}$, the identity morphism in $\mathrm{Mor}_{\mathcal{D}}(F(A), F(A))$;
(4) for all objects A, B, C in $\mathrm{Ob}(\mathcal{C})$ and all morphisms $g\colon A \to B$ in $\mathrm{Mor}_{\mathcal{C}}(A, B)$ and $f\colon B \to C$ in $\mathrm{Mor}_{\mathcal{C}}(B, C)$, we have $F(f \circ g) = F(f) \circ F(g)$; in other words, given a commutative diagram in $\mathcal{C}$



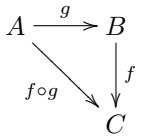
the associated diagram in $\mathcal{D}$ also commutes:



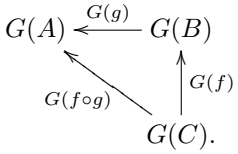
Condition (4) is the "functoriality" of F. Condition (2) (do not reverse the direction of the arrows) is what makes F covariant.

A *contravariant functor* $G\colon \mathcal{C} \to \mathcal{D}$ is a "rule of assignment":

(1) for each object A in $\mathrm{Ob}(\mathcal{C})$, the rule G associates an object $G(A)$ in $\mathrm{Ob}(\mathcal{D})$;
(2) for each morphism $f\colon A \to B$ in $\mathrm{Mor}_{\mathcal{C}}(A, B)$, the rule G associates a morphism $G(f)\colon G(B) \to G(A)$ in $\mathrm{Mor}_{\mathcal{D}}(G(B), G(A))$;
(3) for each object A in $\mathrm{Ob}(\mathcal{C})$, if i_A is the identity morphism in $\mathrm{Mor}_{\mathcal{C}}(A, A)$, then $G(i_A) = i_{G(A)}$, the identity morphism in $\mathrm{Mor}_{\mathcal{D}}(G(A), G(A))$;
(4) for all objects A, B, C in $\mathrm{Ob}(\mathcal{C})$ and all morphisms $g\colon A \to B$ in $\mathrm{Mor}_{\mathcal{C}}(A, B)$ and $f\colon B \to C$ in $\mathrm{Mor}_{\mathcal{C}}(B, C)$, we have $G(f \circ g) = G(g) \circ G(f)$; in other words, given a commutative diagram in $\mathcal{C}$



the associated diagram in $\mathcal{D}$ also commutes:



Condition (4) is the "functoriality" of G. Condition (2) (reverse the direction of the arrows) is what makes D contravariant.

EXAMPLE 2.3. Forgetful functors: we define a rule of association $F\colon \underline{\text{gps}} \to \underline{\text{sets}}$ that associates, to each group G, the underlying set $F(G)$ where we "forget" the group operation. For each homomorphism $f\colon G \to H$ in $\mathrm{Mor}_{\underline{\text{gps}}}(G, H)$, we let $F(f)\colon F(G) \to F(G)$ in $\mathrm{Mor}_{\underline{\text{sets}}}(F(G), F(H))$ denote the underlying set-theoretic function where we "forget" that f respects the groups operations: remember that we have forgot the group structures. This is a covariant functor.

Similar forgetful functors are constructed $\underline{\text{ab}} \to \underline{\text{gps}}$ (forget the commutativity of the operation), $\underline{\text{man}} \to \underline{\text{top}}$ (forget the manifold structure and only remember the topological structure), etc.

EXAMPLE 2.4. The abelianization functor $F\colon \underline{\text{gps}} \to \underline{\text{ab}}$: For each group G, set $F(G) = G/[G, G]$ where $[G, G]$ is the commutator subgroup; see Section 1.9. For each group homomorphism $\varphi\colon G \to H$, Theorem 9.4 implies that the following function is a well-defined abelian group homomorphism: $G/[G, G] \to H/[H, H]$ given by $\overline{g} \mapsto \overline{f(g)}$. Denote this map by $F(\varphi)\colon F(G) \to F(H)$.

This is a covariant functor, as follows. We have verified conditions (1) and (2) from Definition 2.2. It remains to check conditions (3) and (4).

(3) Let $\mathrm{id}_G\colon G \to G$ be the identity homomorphism on a group G. We show that $F(\mathrm{id}_G) = \mathrm{id}_{F(G)}\colon F(G) \to F(G)$: for each $\overline{g} \in F(G) = G/[G, G]$, we have

$$F(\mathrm{id}_G)(\overline{g}) = \overline{\mathrm{id}_G(g)} = \overline{g} = \mathrm{id}_{F(G)}(\overline{g}).$$

(4) Let $\varphi\colon G \to H$ and $\psi\colon H \to K$ be group homomorphisms. We show that $F(\psi \circ \varphi) = F(\psi) \circ F(\varphi)$:

$$F(\psi \circ \varphi)(\overline{g}) = \overline{(\psi \circ \varphi)(g)} = \overline{\psi(\varphi(g))}$$
$$F(\psi) \circ F(\varphi)(\overline{g}) = F(\psi)(F(\varphi)(\overline{g})) = F(\psi)(\overline{\varphi(g)}) = \overline{\psi(\varphi(g))}.$$

EXAMPLE 2.5. Hom functors: Let $\mathcal{C}$ be a category and fix an object A in $\mathcal{C}$.

We define a covariant functor $F_A\colon \mathcal{C} \to \underline{\text{sets}}$. For each object B in $\text{Ob}(\mathcal{C})$, we set $F_A(B) = \text{Mor}_{\mathcal{C}}(A, B)$. For each morphism $f\colon B \to C$ in $\text{Mor}_{\mathcal{C}}(B, C)$, the law of composition yields a function $F_A(f)\colon \text{Mor}_{\mathcal{C}}(A, B) \to \text{Mor}_{\mathcal{C}}(A, C)$ by the rule $g \mapsto f \circ g$; this is how we define $F_A(f)\colon F_A(B) \to F_A(C)$. The fact that $i_B \circ g = g$ for all $G \in \text{Mor}_{\mathcal{C}}(A, B)$ shows that $F_A(i_B) = i_{F_A(B)}$. The associativity of the law of composition justifies the functoriality of F_A: $F_A(f \circ g) = F_A(f) \circ F_A(g)$. In practice we write $\text{Hom}_{\mathcal{C}}(A, -) = F_A$: $\text{Hom}_{\mathcal{C}}(A, B) = F_A(B)$ and $\text{Hom}_{\mathcal{C}}(A, f) = F_A(f)$.

We define a contravariant functor $G_A\colon \mathcal{C} \to \underline{\text{sets}}$. For each object B in $\text{Ob}(\mathcal{C})$, we set $G_A(B) = \text{Mor}_{\mathcal{C}}(B, A)$. For each morphism $f\colon B \to C$ in $\text{Mor}_{\mathcal{C}}(B, C)$, the law of composition yields a function $G_A(f)\colon \text{Mor}_{\mathcal{C}}(C, A) \to \text{Mor}_{\mathcal{C}}(B, A)$ by the rule $g \mapsto g \circ f$; this is how we define $G_A(f)\colon G_A(C) \to G_A(B)$. In practice we write $\text{Hom}_{\mathcal{C}}(A, -) = G_A$: $\text{Hom}_{\mathcal{C}}(A, B) = G_A(B)$ and $\text{Hom}_{\mathcal{C}}(A, f) = G_A(f)$.

EXAMPLE 2.6. A "non-functor": For each group G, let $Z(G)$ denote the center of G. We show that this operation cannot be made into a covariant functor $Z\colon \underline{\text{gps}} \to \underline{\text{ab}}$. Let $h\colon \mathbb{Z}/2\mathbb{Z} \to S_3$ be given by $h(\overline{0}) = (1)$ and $h(\overline{1}) = (1\,2)$. This is a group homomorphism. Let $g\colon S_3 \to S_3/A_3$ be the natural epimorphism, and let $f\colon S_3/A_3 \to \mathbb{Z}/2\mathbb{Z}$ be the (unique) isomorphism. With $f' = f \circ g$, we have $f' \circ h = \text{id}_{\mathbb{Z}/2\mathbb{Z}}$.

Since $\mathbb{Z}/2\mathbb{Z}$ is abelian, we have $Z(\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. On the other hand, we have seen that $Z(S_3) = \{(1)\}$. Suppose that there is a covariant functor $Z\colon \underline{\text{gps}} \to \underline{\text{ab}}$ such that $Z(G)$ is the center of G for each group G. The homomorphisms f' and h yield a commutative diagram in $\underline{\text{gps}}$

$$\begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} & \xrightarrow{h} & S_3 \\ & \searrow^{\text{id}_{\mathbb{Z}/2\mathbb{Z}}} & \downarrow{\scriptstyle f'} \\ & & \mathbb{Z}/2\mathbb{Z}. \end{array}$$

Since Z is a functor, we have a commutative diagram in $\underline{\text{ab}}$

$$\begin{array}{ccc} Z(\mathbb{Z}/2\mathbb{Z}) & \xrightarrow{Z(h)} & Z(S_3) \\ & \searrow^{Z(\text{id}_{\mathbb{Z}/2\mathbb{Z}})} & \downarrow{\scriptstyle Z(f')} \\ & & Z(\mathbb{Z}/2\mathbb{Z}) \end{array} \qquad \begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} & \xrightarrow{Z(h)} & \{0\} \\ & \searrow^{\text{id}_{\mathbb{Z}/2\mathbb{Z}}} & \downarrow{\scriptstyle Z(f')} \\ & & \mathbb{Z}/2\mathbb{Z}. \end{array}$$

Since the target of $Z(h)$ is $\{0\}$, we have $Z(h) = 0$; and similarly, we have $Z(f') = 0$. Hence, the functoriality of Z yields

$$\text{id}_{\mathbb{Z}/2\mathbb{Z}} = Z(\text{id}_{\mathbb{Z}/2\mathbb{Z}}) = Z(f' \circ h) = Z(f') \circ Z(h) = 0 \circ 0 = 0.$$

This is a contradiction, and so there is no way to make Z into a functor.

CHAPTER 3

Ring Theory

1. Day 1

DEFINITION 1.1. A *ring* is a nonempty set R with two binary operations "$+$" and "$\cdot$" such that $(R,+)$ is an abelian group, $(R,\cdot)$ is a semigroup, and $(R,+,\cdot)$ satisfies both distributive laws:

$$r(s+t) = rs + rt \qquad (r+s)t = st + st.$$

A ring R is *commutative* if the multiplication $\cdot$ is commutative.

A ring R has *identity* if there is a (two-sided) multiplicative identity $1_R \in R$. (Note that we do not assume the existence of multiplicative inverses.)

A *field* is a commutative ring with identity $1_R \neq 0_R$ such that every nonzero element in R has a (two-sided) multiplicative inverse in R.

EXAMPLE 1.2. Under the usual addition and multiplication of integers, $\mathbb{Z}$ is a commutative ring with identity; it is not a field.

Under the usual addition and multiplication, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.

Under the usual addition and multiplication of matrices, $M_2(\mathbb{R})$ is a ring with identity that is not commutative. (More generally, this holds for $M_n(R)$ where $n \geqslant 2$ and R is any commutative ring with identity.)

Under the usual addition and multiplication of integers, $2\mathbb{Z}$ is a commutative ring without identity.

EXAMPLE 1.3. Fix an integer $n \geqslant 2$. Define multiplication in $\mathbb{Z}/n\mathbb{Z}$ by the formula $\overline{a} \cdot \overline{b} = \overline{ab}$. (Note that this is well-defined.) Under the usual addition in $\mathbb{Z}/n\mathbb{Z}$, this multiplication endows $\mathbb{Z}/n\mathbb{Z}$ with the structure of a commutative ring with identity. Furthermore, $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime. (Exercise.)

PROPOSITION 1.4. *Let R be a ring.*

(a) *The additive identity in R is unique.*
(b) *If R has (multiplicative) identity, then the multiplicative identity in R is unique.*
(c) *For each $r \in R$, we have $0_R r = 0_R = r 0_R$.*
(d) *Assume that R has identity. Then $R = \{0_R\}$ if and only if $1_R = 0_R$.*

PROOF. (a) and (b): Proposition 1.1.10.

(c) $0r = (0+0)r = 0r + 0r \implies 0 = 0r$. The other equality is verified similarly.

(d) The implication "$\implies$" is immediate. For "$\impliedby$" assume $1 = 0$. For each $r \in R$, we have $r = 1r = 0r = 0$. □

EXAMPLE 1.5. Group rings: Let G be a group with operation written multiplicatively, and let R be a ring with identity. Let $R[G]$ be the group $R^{(G)}$, written

additively. The elements of $R[G]$ are finite formal sums $\sum_{g\in G} r_g g$ with the $r_g \in R$, and addition is given by

$$(\textstyle\sum_{g\in G} r_g g) + (\sum_{g\in G} s_g g) = \sum_{g\in G}(r_g + s_g)g.$$

Define multiplication on $R[G]$ by the formula

$$(\textstyle\sum_{g\in G} r_g g)(\sum_{h\in G} s_h h) = \sum_{g,h\in G}(r_g s_h)(gh).$$

This is a ring with identity $1_{R[G]} = 1_R e_G$. The ring $R[G]$ is commutative if and only if R is commutative and G is abelian. (Exercise.)

DEFINITION 1.6. Let R and S be rings. A function $f\colon R \to S$ is a *homomorphism of rings* or *ring homomorphism* if it respects the addition and multiplication on the rings: for all $r, r' \in R$, we have $f(r+r') = f(r)+f(r')$ and $f(rr') = f(r)f(r')$.

If R and S are rings with identity, then f is a *homomorphism of rings with identity* if it is a ring homomorphism and $f(1_R) = 1_S$.

EXAMPLE 1.7. When $f\colon R \to S$ is a ring homomorphism and the rings R and S both have identity, we may have $f(1_R) \neq 1_S$. For example, this is so for the ring homomorphism $f\colon \mathbb{R} \to M_2(\mathbb{R})$ given by $f(r) = \left(\begin{smallmatrix} r & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

EXAMPLE 1.8. Direct products of rings; see Definition 1.17.8. Let $\{R_\lambda\}_{\lambda\in\Lambda}$ be a nonempty set of nonzero rings.

The product $\prod_\lambda R_\lambda$ is a ring with addition and multiplication defined coordinatewise: $(r_\lambda) + (r'_\lambda) = (r_\lambda + r'_\lambda)$ and $(r_\lambda)(r'_\lambda) = (r_\lambda r'_\lambda)$.

The product $\prod_\lambda R_\lambda$ has identity if and only if each R_λ has identity. $\Longleftarrow$: If $1_{R_\lambda} \in R_\lambda$ is a multiplicative identity, then the sequence (1_{R_λ}) is a multiplicative identity for $\prod_\lambda R_\lambda$. $\Longrightarrow$: If (r_λ) is a multiplicative identity for $\prod_\lambda R_\lambda$, then r_λ is a multiplicative identity for R_λ.

Similarly, the product $\prod_\lambda R_\lambda$ is commutative if and only if each R_λ is commutative.

2. Day 2

PROPOSITION 2.1. *Let R be a ring and let $r, s, t \in R$.*

(a) *If $r + s = r + t$, then $s = t$.*
(b) *r has a unique additive inverse in R, denoted $-r$.*
(c) *$-(-r) = r$.*
(d) *$(-r)s = -(rs) = r(-s)$.*
(e) *If R has identity, then $(-1_R)r = -r = r(-1_R)$.*
(f) *$(-r)(-s) = rs$.*
(g) *For all $a_1, \ldots, a_m, b_1, \ldots, b_n \in R$, we have*

$$(\textstyle\sum_{i=1}^m a_i)(\sum_{j=1}^n b_j) = \sum_{i=1}^m \sum_{j=1}^n a_i b_j.$$

PROOF. (a) Exercise 1.1.14(a).

(b) Exercise 1.1.14(c).

(c) $r + (-r) = 0$, so r satisfies the defining property for $-(-r)$. Now use part (b).

(d) $rs + (-r)s = (r + (-r))s = 0s = 0$. This explains the first equality, and the second one is explained similarly.

(e) $-r = -(1r) = (-1)r$ by part (d). This explains the first equality, and the second one is explained similarly.

(f) $(-r)(-s) = r(-(-s)) = rs$.

(g) First, we show $a(\sum_{j=1}^{n} b_j) = (\sum_{j=1}^{n} ab_j)$ by induction on n: For $n \geqslant 2$, we have

$$a(\textstyle\sum_{j=1}^{n} b_j) = a(b_1 + \sum_{j=2}^{n} b_j) = ab_1 + a\sum_{j=2}^{n} b_j) = ab_1 + \sum_{j=2}^{n} ab_j) = (\sum_{j=1}^{n} ab_j).$$

Next, we show $(\sum_{i=1}^{m} a_i)(\sum_{j=1}^{n} b_j) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$ by induction on m. The base case $m = 1$ is in the previous paragraph. For $m \geqslant 2$, we have

$$\begin{aligned}(\textstyle\sum_{i=1}^{m} a_i)(\sum_{j=1}^{n} b_j) &= (a_1 + \sum_{i=2}^{m} a_i)(\sum_{j=1}^{n} b_j)\\ &= a_1(\textstyle\sum_{j=1}^{n} b_j) + (\sum_{i=2}^{m} a_i)(\sum_{j=1}^{n} b_j)\\ &= \textstyle\sum_{j=1}^{n} a_1 b_j + \sum_{i=2}^{m}\sum_{j=1}^{n} a_i b_j\\ &= \textstyle\sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j.\end{aligned}$$

□

DEFINITION 2.2. Let R be a ring. For $r, s \in R$, define $r - s = r + (-s)$.

A subset $S \subseteq R$ is a *subring* if it is a ring with respect to the addition, subtraction, and multiplication on R.

EXAMPLE 2.3. $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.

EXAMPLE 2.4. Let $S = \{ \left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right) \in M_2(\mathbb{R}) | \, r \in \mathbb{R}\} \subset M_2(\mathbb{R})$. Then S is a subring of $M_2(\mathbb{R})$.

REMARK 2.5. If S is a subring of R, then $0_S = 0_R$ as follows: $s \in S \implies 0_R = s - s \in S$, and since 0_R is an additive identity on R it is also an additive identity on S.

EXAMPLE 2.6. Let $S = \{ \left(\begin{smallmatrix} r & 0 \\ 0 & 0 \end{smallmatrix}\right) \in M_2(\mathbb{R}) | \, r \in \mathbb{R}\} \subset M_2(\mathbb{R})$. Then S is a subring of $M_2(\mathbb{R})$. Note that S and $M_2(\mathbb{R})$ are both rings with identity, but they do not have the same identity.

PROPOSITION 2.7. *(Subring test) Let R be a ring and $S \subseteq R$ a subset. Then S is a subring of R if and only if it satisfies the following conditions:*

(1) *$S \neq \emptyset$;*
(2) *S is closed under the subtraction from R;*
(3) *S is closed under the multiplication from R.*

PROOF. Like the subgroup test, Proposition 1.4.2. □

PROPOSITION 2.8. *If $f\colon R \to T$ is a ring homomorphism, then $\mathrm{Im}(f)$ is a subring of T.*

PROOF. Use the Subring Test as in the proof of Exercise 1.3.8(a). □

DEFINITION 2.9. Let R be a ring. A subset $I \subseteq R$ is a *(two-sided) ideal* if $(I, +) \leqslant (R, +)$ and, for all $a \in I$ and all $r \in R$, we have $ar \in I$ and $ra \in I$. In particular, when I is a two-sided ideal of R, the quotient R/I is a well-defined additive abelian group.

EXAMPLE 2.10. For each integer n, the set $n\mathbb{Z}$ is a two-sided ideal in $\mathbb{Z}$.

In $\mathbb{Q}$, the set $\mathbb{Z}$ is a subring; it is not an ideal.

The only ideals of $\mathbb{Q}$ are $\{0\}$ and $\mathbb{Q}$. More generally, if k is a field, then the only two-sided ideals of k are $\{0\}$ and k. (Exercise.)

REMARK 2.11. If I is an ideal in R, then $0_R \in I$ because $s \in S \implies 0_R = s - s \in S$.

PROPOSITION 2.12. *(Ideal test) Let R be a ring and $I \subseteq R$ a subset. Then I is an ideal of R if and only if it satisfies the following conditions:*

(1) *$I \neq \emptyset$;*
(2) *I is closed under the subtraction from R;*
(3) *For all $r \in R$ and all $a \in I$, we have $ra \in I$ and $ar \in I$.*

PROOF. Like the Subring Test. □

PROPOSITION 2.13. *If $f\colon R \to T$ is a ring homomorphism, then $\operatorname{Ker}(f)$ is an ideal of R.*

PROOF. Use the Ideal Test as in the proof of Exercise 1.3.8(a). □

PROPOSITION 2.14. *Let R be a ring and $I \subseteq R$ a two-sided ideal.*

(a) *Define a product on the quotient R/I by the formula $\overline{r} \cdot \overline{s} = \overline{rs}$. This is well-defined and makes R/I into a ring.*
(b) *If R is commutative, then so is R/I.*
(c) *If R has identity 1_R, then R/I has identity $1_{R/I} = \overline{1_R}$.*
(d) *The natural map $\pi\colon R \to R/I$ given by $r \mapsto \overline{r}$ is a surjective ring homomorphism with kernel I.*
(e) *If R has identity, then π is a homomorphism of rings with identity.*

PROOF. (a) If $\overline{r} = \overline{r'}$ and $\overline{s} = \overline{s'}$, then $r - r', s - s' \in I$ and so

$$rs - r's' = rs - r's + r's - r's' = \underbrace{\underbrace{\underbrace{(r-r')}_{\in I}\, s}_{\in I} + \underbrace{r' \underbrace{(s-s')}_{\in I}}_{\in I}}_{\in I} \in I$$

which implies $\overline{rs} = \overline{r's'}$. The remaining properties of R/I follow from the corresponding properties for R. For instance, once half of distributivity:

$$\overline{r}(\overline{s} + \overline{t}) = \overline{r(s+t)} = \overline{rs + rt} = \overline{rs} + \overline{r}\overline{t}.$$

(b) See Exercises 2.
(c) $\overline{1}\overline{r} = \overline{1r} = \overline{r}$ etc.
(d) π is a well-defined surjective additive abelian group homomorphism by Example 1.4.1(a). And it is a ring homomorphism because $\pi(rs) = \overline{rs} = \overline{r} \cdot \overline{s} = \pi(r)\pi(s)$.
(e) $1_{R/I} = \overline{1_R} = \pi(1_R)$. □

PROPOSITION 2.15 (First Isomorphism Theorem). *Let $f\colon R \to S$ be a ring homomorphism.*

(a) *The function $\overline{f}\colon R/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ given by $\overline{r} \mapsto f(r)$ is a well-defined isomorphism of rings and so $\operatorname{Im}(f) \cong R/\operatorname{Ker}(f)$.*
(b) *f is a monomorphism if and only if $\operatorname{Ker}(f) = \{0_R\}$.*

PROOF. As in Exercise 1.3.8. □

3. Day 3

Here is the ideal correspondence for quotients, and the third isomorphism theorem.

THEOREM 3.1. *Let R be a ring and $I \subseteq R$ an ideal. Let $\pi\colon R \to R/I$ be the ring epimorphism $\pi(r) = \overline{r}$. There is a 1-1 correspondence*

$$\{\textit{ideals } J \subseteq R \mid I \subseteq J\} \longleftrightarrow \{\textit{ideals } J' \subseteq R/I\}$$

given by

$$J \longmapsto J/I$$
$$\pi^{-1}(J') \longmapsfrom J'$$

If J is an ideal of R such that $I \subseteq J$, then the function $\tau\colon R/I \to R/J$ given by $\tau(r+I) = r+J$ is a well-defined ring epimorphism with $\mathrm{Ker}(\tau) = J/I$; in particular, there is a (well-defined) ring isomorphism $(R/I)/(J/I) \xrightarrow{\cong} R/J$.

PROOF. As in Theorems 1.6.6 and 1.6.10. □

EXAMPLE 3.2. Let $n \geqslant 2$. The ideals of $\mathbb{Z}/n\mathbb{Z}$ are exactly the sets of the form $m\mathbb{Z}/n\mathbb{Z} = \{\overline{a} \mid m\big|a\}$ for some $m\big|n$. And $(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$.

Here are three important ways to combine ideals.

PROPOSITION 3.3. *If $\{I_\lambda\}_{\lambda\in\Lambda}$ is a nonempty set of ideals in a ring R, then $\cap_{\lambda\in\Lambda} I_\lambda$ is an ideal in R. In particular, if I, J are ideals of R, then so is $I \cap J$.*

PROOF. As in Exercise 1.3.9. □

EXAMPLE 3.4. If $m, n \in \mathbb{Z}$, then $m\mathbb{Z} \cap n\mathbb{Z} = \mathrm{lcm}(m,n)\mathbb{Z}$.

DEFINITION 3.5. Let X be a subset of a ring R. The *ideal generated by X* is the intersection of all ideals of R containing X; it is denoted (X). If $X = \{x_1, \ldots, x_n\}$, then we write $(X) = (x_1, \ldots, x_n)$.

PROPOSITION 3.6. *Let X be a subset of a ring R.*

(a) *The set (X) is an ideal of R that contains X.*
(b) *(X) is the smallest ideal of R containing X.*
(c) *Assume that R has identity. Then*

$$(X) = \{\textit{finite sums of the form } \textstyle\sum_i \sum_j a_{i,j} x_i b_{i,j} \mid a_{i,j}, b_{i,j} \in R \textit{ and } x_i \in X\}.$$

In particular, if $x \in R$, then

$$(x) = \{\textit{finite sums of the form } \textstyle\sum_j a_j x b_j \mid a_j, b_j \in R\}.$$

(d) *Assume that R is commutative and has identity. Then*

$$(X) = \{\textit{finite sums of the form } \textstyle\sum_i c_i x_i \mid c_i \in R \textit{ and } x_i \in X\}.$$

In particular, if $x \in R$, then

$$(x) = \{cx \mid c \in R\}.$$

PROOF. (a) The set of all ideals of R containing X is nonempty because R is an ideal of R containing X. Now apply Proposition 3.3.

(b) If J is an ideal of R containing X, then J is one of the ideals in the intersection defining (X). Hence $(X) \subseteq J$.

(c) For the first equality, set

$$I = \{\text{finite sums of the form } \textstyle\sum_i \sum_j a_{i,j} x_i b_{i,j} \mid a_{i,j}, b_{i,j} \in R \text{ and } x_i \in X\}.$$

We need to show $(X) = I$.

"$\supseteq$" For each ideal J containing X, the fact that J is an ideal implies that every finite sum of the form $\sum_i \sum_j a_{i,j} x_i b_{i,j}$ is in J. In particular, every such sum is in the intersection of all the ideals of R containing X. Hence, the containment.

"$\subseteq$" It is straightforward to show that I is an ideal of R. Because R has identity, we have $X \subseteq I$. Hence, I is one of the ideals in the intersection defining (X), and so $(X) \subseteq I$.

The second equality is a special case of the first one.

(d) The first equality follows from part (c) and the following computation:

$$\textstyle\sum_i \sum_j a_{i,j} x_i b_{i,j} = \sum_i \sum_j (a_{i,j} b_{i,j} x_i) = \sum_i (\underbrace{\sum_j a_{i,j} b_{i,j}}_{c_i}) x_i.$$

The first equality uses the commutativity of R, and the second one uses the generalized distributive law from Proposition 2.1(g).

The second equality is a special case of the first one. □

EXAMPLE 3.7. In $\mathbb{Z}$, we have $(n) = n\mathbb{Z}$. If $m, n \in \mathbb{Z}$, then $(m, n) = \gcd(m, n)\mathbb{Z}$.

DEFINITION 3.8. Let $I_1, \ldots, I_n$ be ideals of a ring R. Their *sum* is

$$\textstyle\sum_j I_j = I_1 + \cdots + I_n = \{\sum_j a_j \mid a_j \in I_j, j = 1, \ldots, n\}.$$

In particular, for ideals I and J, we set

$$I + J = \{a + b \mid a \in I, b \in J\}.$$

PROPOSITION 3.9. *Let $I_1, \ldots, I_n$ be ideals of a ring R.*

(a) *The sum $\sum_j I_j$ is an ideal of R.*
(b) *The sum $\sum_j I_j$ contains I_k for each $k = 1, \ldots, n$*
(c) *We have $\sum_j I_j = (\cup_j I_j)$. In particular, $\sum_j I_j$ is the smallest ideal of R containing $\cup_j I_j$.*
(d) *For ideals I, J, K in R, we have $(I + J) + K == I + J + K = I + (J + K)$.*

PROOF. (a) Use the ideal test and the generalized distributive law.

(b) Use the fact that $0_R \in I_k$ for each k.

(c) Let $z \in \sum_j I_j$. Then there exist $a_j \in I_j$ such that $z = \sum_j a_j$. Each $a_j \in \cup_j I_j \subseteq (\cup_j I_j)$, so the fact that $(\cup_j I_j)$ is closed under sums implies $z = \sum_j a_j \in (\cup_j I_j)$. Hence $\sum_j I_j \subseteq (\cup_j I_j)$.

For the reverse containment, note that $\sum_j I_j \supseteq I_l$ for each l, and therefore $\sum_j I_j \subseteq \cup_j I_j$. Since $(\cup_j I_j)$ is the smallest ideal containing $\cup_j I_j$, it follows that $\sum_j I_j \supseteq (\cup_j I_j)$.

The second statement follows from the first one by Proposition 3.6(b).

(d) This follows from the associativity and (generalized) commutativity of addition. □

EXAMPLE 3.10. In $\mathbb{Z}$, we have $m\mathbb{Z} + n\mathbb{Z} = (m, n) = \gcd(m, n)\mathbb{Z}$.

DEFINITION 3.11. Let $I_1, \ldots, I_n$ be ideals of a ring R. Their *product* is

$$\begin{aligned}\textstyle\prod_j I_j &= I_1 \cdots I_n \\ &= \{\text{finite sums of elements of the form } a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\}.\end{aligned}$$

In particular, for ideals I and J, we set

$$IJ = \{\text{finite sums of elements of the form } ab \mid a \in I, b \in J\}.$$

4. Day 4

PROPOSITION 4.1. *Let $I_1, \ldots, I_n$ be ideals of a ring R.*

(a) *The product $\prod_j I_j$ is an ideal of R.*
(b) *We have $\prod_j I_j = (\{a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\})$. In particular, $\prod_j I_j$ is the smallest ideal of R containing the set $\{a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\}$.*
(c) *For ideals I, J, K in R, we have $(IJ)K = I(JK) = IJK$.*
(d) *If J is an ideal of R, then $J(\sum_j I_j) = \sum_j (JI_j)$ and $(\sum_j I_j)J = \sum_j (I_j J)$.*
(e) *If R is commutative and $\sigma \in S_n$, then $\prod_j I_j = \prod_j I_{\sigma(j)}$.*

PROOF. (a) Use the ideal test and the generalized distributive law.

(b) Let $c_j \in I_j$ for $j = 1, \ldots, n$. Then

$$\begin{aligned}c_1 \cdots c_n &\in \{a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\} \\ &\subseteq (\{a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\}) = J.\end{aligned}$$

Since $(\{a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\})$ is closed under finite sums, it follows that every finite sum of elements of the form $c_1 \cdots c_n$ is in J. From the definition of $\prod_j I_j$, we conclude $\prod_j I_j \subseteq J$.

On the other hand, $\prod_j I_j$ is an ideal that contains each product $c_1 \cdots c_n$ with $c_j \in I_j$. Since J is the smallest such ideal, it follows that $\prod_j I_j \supseteq J$.

The second statement follows from the first one by Proposition 3.6(b).

(c) Check $(IJ)K \subseteq IJK$ directly from the definitions using associativity of multiplication. Check $(IJ)K \supseteq IJK$ by showing that every generator of IJK is in $(IJ)K$. The equality $I(JK) = IJK$ is verified similarly.

(d) To show $J(\sum_j I_j) \subseteq \sum_j (JI_j)$, show that every generator of $J(\sum_j I_j)$ is in $\sum_j (JI_j)$. For $J(\sum_j I_j) \supseteq \sum_j (JI_j)$, show directly that every element of $\sum_j (JI_j)$ is in $J(\sum_j I_j)$ using the (generalized) distributive law. The equality $(\sum_j I_j)J = \sum_j (I_j J)$ is verified similarly.

(e) This follows similarly from the (generalized) commutative law. □

EXAMPLE 4.2. If $m, n \in \mathbb{Z}$, then $(m\mathbb{Z})(n\mathbb{Z}) = mn\mathbb{Z}$.

DEFINITION 4.3. Let R be a ring and $P \subseteq R$ an ideal. P is *prime* if $P \neq R$ and, for all ideals $I, J \subseteq R$, if $IJ \subseteq P$, then either $I \subseteq P$ or $J \subseteq P$.

EXAMPLE 4.4. $0\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. If $0 \neq m \in \mathbb{Z}$, then $m\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ if and only if m is a prime number. (These are the prototypes.)

PROPOSITION 4.5. *Let R be a ring and $P \subsetneq R$ an ideal.*

(a) *Assume that, for all $a, b \in R$, if $ab \in P$, then either $a \in P$ or $b \in P$. Then P is prime.*

(b) *If R is commutative and P is prime, then, for all $a, b \in R$, if $ab \in P$, then either $a \in P$ or $b \in P$.*

PROOF. (a) Let $I, J \subseteq R$ be ideals such that $IJ \subseteq P$ and $I \not\subseteq P$. We need to show that $J \subseteq P$. Let $a \in I - P$. For all $b \in J$, we have $ab \in IJ \subseteq P$; since $a \notin P$, our hypothesis implies $b \in P$. Thus, $J \subseteq P$.

(b) Let $a, b \in R$ and assume that $ab \in P$. Since P is an ideal, we have $(ab) \subseteq P$. Since R is commutative, we have $(a)(b) = (ab) \subseteq P$; Exercise. Since P is prime, either $(a) \subseteq P$ or $(b) \subseteq P$, and so either $a \in P$ or $b \in P$. □

DEFINITION 4.6. An *integral domain* is a nonzero commutative ring with identity such that, for all $0 \neq a, b \in R$ we have $ab \neq 0$.

EXAMPLE 4.7. $\mathbb{Z}$ is an integral domain. Every field is an integral domain, e.g., $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

PROPOSITION 4.8. *Let R be a nonzero commutative ring with identity. An ideal $I \subseteq R$ is prime if and only if R/I is an integral domain.*

PROOF. " $\Longrightarrow$ " Assume that I is prime. Then $I \subsetneq R$ and so $R/I \neq 0$. Also, because R is commutative with identity, so is R/I. Let $0 \neq a + I, b + i \in R/I$. Then $a, b \notin I$ and so $ab \notin I$ because I is prime. Hence $(a + I)(b + I) = ab + I \neq 0$ and so R/I is an integral domain.

" $\Longleftarrow$ " Assume R/I is an integral domain. In particular, we have $R/I \neq 0$ and so $I \subsetneq R$. Let $a, b \in R - P$. Then $0 \neq a + I, b + I \in R/I$. Since R/I is an integral domain, we have $0 \neq (a + I)(b + I) = ab + I$ and so $ab \notin I$. Proposition 4.5(a) implies that I is prime. □

DEFINITION 4.9. An ideal $\mathfrak{m} \subseteq R$ is *maximal* if $\mathfrak{m} \neq R$ and $\mathfrak{m}$ is a maximal element in the set of all proper ideals, partially ordered by inclusion. In other words, $\mathfrak{m}$ is maximal if and only if $\mathfrak{m} \neq R$ and, for all ideals $I \subseteq R$, if $\mathfrak{m} \subseteq I$, then either $I = \mathfrak{m}$ or $I = R$.

EXAMPLE 4.10. $0\mathbb{Z}$ and $6\mathbb{Z}$ are not maximal ideals of $\mathbb{Z}$ because $0\mathbb{Z} \subsetneq 6\mathbb{Z} \subsetneq 3\mathbb{Z} \subsetneq \mathbb{Z}$. In fact, $m\mathbb{Z}$ is maximal if and only if m is prime.

5. Day 5

PROPOSITION 5.1. *Let R be a nonzero ring with identity. For every ideal $I \subsetneq R$, there is a maximal ideal $\mathfrak{m} \subsetneq R$ such that $I \subseteq \mathfrak{m}$. In particular, R has at least one maximal ideal.*

PROOF. Fix an ideal $I \subsetneq R$. We use Zorn's Lemma to show that I is contained in some maximal ideal $\mathfrak{m}$ of R. Let $\mathcal{A}$ denote the set of all ideals J such that $I \subseteq J \subsetneq R$. Partially order $\mathcal{A}$ by inclusion. Since $I \neq R$, we have $I \in \mathcal{A}$ and so $\mathcal{A} \neq \emptyset$. In order to be able to invoke Zorn's lemma, we need to show that every chain $\mathcal{C}$ in $\mathcal{A}$ has an upper bound in $\mathcal{A}$.

Let $K = \cup_{J \in \mathcal{C}} J$. We will be done once we show that K is an ideal of R such that $K \neq R$. Indeed, then $K \supseteq J \supseteq I$ for all $J \in \mathcal{C}$ and so $K \in \mathcal{A}$ and K is an upper bound for $\mathcal{C}$ in $\mathcal{A}$.

We use the ideal test to show that K is an ideal of R. Since $0 \in I \subseteq K$, we have $K \neq \emptyset$. Let $a, a' \in K = \cup_{J \in \mathcal{C}} J$. Then there are $J, J' \in \mathcal{C}$ such that $a \in J$ and $a' \in J'$. Since $\mathcal{C}$ is a chain, either $J \subseteq J'$ or $J' \subseteq J$. Assume without loss of generality that $J \subseteq J'$. Then $a, a' \in J'$ and so $a - a' \in J' \subseteq K$ since J' is an ideal.

Now let $r \in R$ and $b \in K$. There is an ideal $J'' \in \mathcal{C}$ such that $b \in J''$. Since J'' is an ideal, we have $rb \in J'' \subseteq K$. Similarly, we see that $br \in K$, and so K is an ideal.

Suppose $K = R$. Then $1_R \in K$. It follows that $1_R \in J'''$ for some $J''' \in \mathcal{C}$ and so $J''' = R$ by an exercise. This contradicts the fact that $J''' \in \mathcal{C}$.

Zorn's Lemma implies that $\mathcal{C}$ has a maximal element $\mathfrak{m}$. It is straightforward to check that $\mathfrak{m}$ is a maximal ideal of R that contains I.

For the final statement, note that $(0) \neq R$ and so (0) is contained in some maximal ideal $\mathfrak{m}'$. Hence, R has at least one maximal ideal. □

PROPOSITION 5.2. *Let R be a nonzero commutative ring with identity.*

(a) *An ideal I is maximal if and only if R/I is a field.*
(b) *Every maximal ideal of R is prime.*

PROOF. (a) If I is maximal, then there are no ideals J such that $I \subsetneq J \subsetneq R$. The ideal correspondence shows that R/I has only two ideals, I/I and R/I. Hence, R/I is a field by an exercise.

Conversely, assume that R/I is a field and let J be an ideal such that $I \subseteq J \subseteq R$. Hence, J/I is an ideal of R/I. Since R/I is a field, the same exercise shows that R/I has only two ideals, I/I and R/I. Hence, either $J/I = I/I$ or $J/I = R/I$. That is, either $J = I$ or $J = R$, so I is maximal.

(b) If $\mathfrak{m} \subsetneq R$ is a maximal ideal, then $R/\mathfrak{m}$ is a field. Hence, $R/\mathfrak{m}$ is an integral domain and so $\mathfrak{m}$ is prime. □

PROPOSITION 5.3. *Let R be a nonzero commutative ring with identity. Let $I \subsetneq R$ be an ideal and let $\pi\colon R \to R/I$ be the ring epimorphism $\pi(r) = \overline{r}$.*

(a) *There is a 1-1 correspondence*

$$\{\textit{prime ideals } P \subsetneq R \mid I \subseteq P\} \longleftrightarrow \{\textit{prime ideals } P' \subsetneq R/I\}$$

given by

$$P \longmapsto P/I$$
$$\pi^{-1}(P') \longmapsfrom P'.$$

In other words, the ideal $J/I \subseteq R/I$ is prime if and only if J is a prime ideal of R.

(b) *There is a 1-1 correspondence*

$$\{\textit{maximal ideals } \mathfrak{m} \subsetneq R \mid I \subseteq \mathfrak{m}\} \longleftrightarrow \{\textit{maximal ideals } \mathfrak{m}' \subsetneq R/I\}$$

given by

$$\mathfrak{m} \longmapsto \mathfrak{m}/I$$
$$\pi^{-1}(\mathfrak{m}') \longmapsfrom \mathfrak{m}'.$$

In other words, the ideal $J/I \subseteq R/I$ is maximal if and only if J is a maximal ideal of R.

PROOF. (a) Using the ideal correspondence, it suffices to verify the last statement. The ideal $J/I \subseteq R/I$ is prime if and only if $(R/I)/(J/I) \cong R/J$ is an integral domain, and this is so if and only if J is prime. The isomorphism comes from the Third Isomorphism Theorem.

(b) As in part (a), changing "prime" to "maximal" and "integral domain" to "field". □

EXAMPLE 5.4. The prime ideals of $\mathbb{Z}/42\mathbb{Z}$ are $2\mathbb{Z}/42\mathbb{Z}, 3\mathbb{Z}/42\mathbb{Z}, 7\mathbb{Z}/42\mathbb{Z}$ because $42 = (2)(3)(7)$. These are exactly the maximal ideals of $\mathbb{Z}/42\mathbb{Z}$ as well.

Next: Chinese Remainder Theorem. But first, a lemma.

LEMMA 5.5. *Let R be a nonzero commutative ring with identity, and fix ideals $I_1, \ldots, I_n \subseteq R$. If $I_j + I_k = R$ for all $j \neq k$, then $I_j + \cap_{k \neq j} I_k = R$ for all j.*

PROOF. We prove the case $j = 1$; the other cases are obtained by rearranging. Assume without loss of generality that $n \geqslant 3$.

We prove that $I_1 + \cap_{k=2}^{l} I_k = R$ by induction on l. (The case $l = n$ will give the desired result.) The base case $l = 2$ holds by assumption. Assume $l \geqslant 3$ and $I_1 + \cap_{k=2}^{l-1} I_k = R$. The induction hypothesis implies that there exist $a \in I_1$ and $b \in \cap_{k=2}^{l-1} I_k$ such that $1 = a + b$. Our assumption implies that there exist $a' \in I_1$ and $b' \in I_l$ such that $1 = a' + b'$. Since $a, a' \in I_1$, we have $aa', ab', a'b \in I_1$ and so $aa' + ab' + a'b \in I_1$. Since $b \in \cap_{k=2}^{l-1} I_k$ we have $bb' \in \cap_{k=2}^{l-1} I_k$; and since $b' \in I_l$, we have $bb' \in I_l$; hence $bb' \in \cap_{k=2}^{l} I_k$ Hence, we have

$$1 = 1 \cdot 1 = (a+b)(a'+b') = \underbrace{(aa' + ab' + a'b)}_{\in I_1} + \underbrace{bb'}_{\in \cap_{k=2}^{l} I_k} \in I_1 + \cap_{k=2}^{l} I_k$$

and it follows that $I_1 + \cap_{k=2}^{l} I_k = R$. □

EXAMPLE 5.6. For instance, the lemma says that $3\mathbb{Z} + (5\mathbb{Z} \cap 7\mathbb{Z}) = \mathbb{Z}$ because $3\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$ and $3\mathbb{Z} + 7\mathbb{Z} = \mathbb{Z}$.

THEOREM 5.7 (Chinese Remainder Theorem, version 1). *Let R be a nonzero commutative ring with identity, and let $I_1, \ldots, I_n$ be ideals of R.*

(a) *The function $\theta\colon R/(\cap_{j=1}^{n} I_j) \to \prod_{j=1}^{n} R/I_j$ given by $\overline{r} \mapsto (r + I_1, \ldots, r + I_n)$ is well-defined. Furthermore, it is a 1-1 homomorphism of rings with identity.*
(b) *If $I_j + I_k = R$ for all $j \neq k$, then θ is an isomorphism and $\cap_{j=1}^{n} I_j = \prod_{j=1}^{n} I_j$.*

PROOF. (a) The map $\Phi\colon R \to \prod_{j=1}^{n} R/I_j$ given by $r \mapsto (r + I_1, \ldots, r + I_n)$ is a well-defined homomorphism of rings with identity. From the definition, it follows that $\mathrm{Ker}(\Phi) = \cap_{j=1}^{n} I_j$. Hence, the result follows from the First Isomorphism Theorem.

(b) For the first conclusion, it suffices to show that Φ is surjective. Let $(r_1 + I_1, \ldots, r_n + I_n) \in \prod_{j=1}^{n} R/I_j$. For each $j = 1, \ldots, n$, the previous lemma shows that there exist $a_j \in I_j$ and $b_j \in \cap_{k \neq j} I_k$ such that $r_j = a_j + b_j$. Since $a_j \in I_j$, we have $r_j + I_j = b_j + I_j$. For $l \neq j$, since $b_j \in \cap_{k \neq j} I_k \subseteq I_l$, we have $b_j + I_l = 0 + I_l$. With $b = b_1 + \ldots + b_n$ it follows that $b + I_j = r_j + I_j$ for each j, and so $\Phi(b) = (r_1 + I_1, \ldots, r_n + I_n)$.

For the second conclusion, we argue by induction on n. The case $n = 1$ is trivial, so assume that $n \geqslant 2$ and $\cap_{j=1}^{n-1} I_j = \prod_{j=1}^{n-1} I_j$. From the previous lemma,

we know $R = \cap_{j=1}^{n-1} I_j + I_n = \prod_{j=1}^{n-1} I_j + I_n$, and so

$$\begin{aligned}
\cap_{j=1}^{n} I_j &= (\cap_{j=1}^{n-1} I_j) \cap I_n \\
&= (\prod_{j=1}^{n-1} I_j) \cap I_n \\
&= R[(\prod_{j=1}^{n-1} I_j) \cap I_n] \\
&= [\prod_{j=1}^{n-1} I_j + I_n][(\prod_{j=1}^{n-1} I_j) \cap I_n] \\
&= [\prod_{j=1}^{n-1} I_j][(\prod_{j=1}^{n-1} I_j) \cap I_n] + [I_n][(\prod_{j=1}^{n-1} I_j) \cap I_n] \\
&\subseteq [\prod_{j=1}^{n-1} I_j][I_n] + [I_n][(\prod_{j=1}^{n-1} I_j)] \\
&\subseteq [\prod_{j=1}^{n} I_j] + [(\prod_{j=1}^{n} I_j)] \\
&= \prod_{j=1}^{n} I_j.
\end{aligned}$$

From a homework exercise, we know $\prod_{j=1}^{n} I_j \subseteq \cap_{j=1}^{n} I_j$ so we have equality. □

6. Day 6

DEFINITION 6.1. If I is an ideal in R, we write $a \equiv b \pmod{I}$ if $a - b \in I$. This is an equivalence relation on R.

COROLLARY 6.2 (Chinese Remainder Theorem, version 2). *Let R be a nonzero commutative ring with identity, and let $I_1, \ldots, I_n$ be ideals of R such that $I_j + I_k = R$ for all $j \neq k$. For all $r_1, \ldots, r_n \in R$ there exists $b \in R$ such that $b \equiv r_j \pmod{I_j}$ for $j = 1, \ldots, n$. Furthermore, b is uniquely determined up to congruence modulo the ideal $\cap_{j=1}^{n} I_j = \prod_{j=1}^{n} I_j$.*

PROOF. The first statement is a reformulation of the surjectivity of θ in the previous theorem. The second statement corresponds to the injectivity of θ. □

The "traditional" Chinese Remainder Theorem is the special case where $R = \mathbb{Z}$. Note that the proof of Theorem 5.7(b) gives an algorithm for solving a system of congruences.

COROLLARY 6.3 (Chinese Remainder Theorem, version 2). *Let $m_1, \ldots, m_n \in \mathbb{Z}$ such that $\gcd(m_j, m_k) = 1$ for each $j \neq k$. For all $r_1, \ldots, r_n \in \mathbb{Z}$ there exists $b \in \mathbb{Z}$ such that $b \equiv r_j \pmod{m_j}$ for $j = 1, \ldots, n$. Furthermore, b is uniquely determined up to congruence modulo $m = m_1 \cdots m_n$.* □

Here is one way that integral domains are like fields. Note that we are not assuming that a has a multiplicative inverse.

PROPOSITION 6.4. *Let R be an integral domain. If $a, b, c \in R$ such that $ab = ac$, then either $a = 0$, then $b = c$.*

PROOF. $ab = ac$ implies $a(b - c) = 0$. Since R is an integral domain, either $a = 0$ or $b - c = 0$. □

DEFINITION 6.5. Let R be a nonzero commutative ring with identity. An element $u \in R$ is a *unit* if it has a multiplicative inverse in R. An element $p \in R$ is *prime* if it is a nonzero nonunit and (p) is a prime ideal in R. An element $q \in R$ is *irreducible* if it is a nonzero nonunit and, q has only trivial factors, that is, for all $a, b \in R$, if $q = ab$ then either a or b is a unit.

For elements $a, b \in R$, we say *a is a factor of b* or *a divides b* if there exists $c \in R$ such that $b = ac$; when a divides b, we write $a|b$.

An ideal I is *principal* if it can be generated by a single element, that is, if there exists an element $r \in R$ such that $I = (r)$.

EXAMPLE 6.6. The units in $\mathbb{Z}$ are ± 1. The prime elements are exactly the prime numbers (positive and negative), and same for the irreducible elements.

In a field, every nonzero element is a unit. Hence, a field has no prime elements and no irreducible elements.

In $\mathbb{Z}/(6)$, the units are $\overline{1}, \overline{5} = -\overline{1}$; the prime elements are $\overline{2}, \overline{3}, \overline{4} = -\overline{2}$. The element $\overline{2}$ is not irreducible because $\overline{2} = \overline{2} \cdot \overline{4}$. The element $\overline{3}$ is not irreducible because $\overline{3} = \overline{3} \cdot \overline{3}$. The element $\overline{4}$ is not irreducible because $\overline{4} = \overline{2} \cdot \overline{2}$.

EXERCISE 6.7. Let R be a nonzero commutative ring with identity, and let $a, b \in R$. The following conditions are equivalent:

(a) $a|b$;
(b) $b \in (a)$;
(c) $(b) \subseteq (a)$.

PROPOSITION 6.8. *Let R be a nonzero commutative ring with identity. Let $x \in R$ be a nonzero nonunit. Then x is prime if and only if, for all $a, b \in R$, if $p|ab$, then $p|a$ or $p|b$.*

PROOF. From the characterization of prime ideals from Proposition 4.5: (p) is prime if and only if for all $a, b \in R$, if $ab \in (p)$, then either $a \in (p)$ or $b \in (p)$. Now use Exercise 6.7. □

7. Day 7

PROPOSITION 7.1. *Let R be an integral domain. If $p \in R$ is prime, then p is irreducible.*

PROOF. Assume that p is prime, and suppose $p = ab$ for some $a, b \in R$. Then $p|ab$, so the fact that p is prime implies $p|a$ or $p|b$. Assume $p|a$; we need to show that b is a unit. Since $p|a$ and $a|p$, we have $(a) = (p) = (ab)$. Since R is an integral domain, an exercise implies that b is a unit. □

REMARK 7.2. Example 6.6 shows that the assumption "R is an integral domain" is necessary: In $\mathbb{Z}/(6)$, the element $\overline{2}$ is prime but not irreducible.

EXAMPLE 7.3. Not every irreducible element is prime, even in an integral domain. To see this, let $\mathbb{R}[x^2, x^3]$ be the set of polynomials of the form $a_0 + a_2x^2 + a_3x^3 + a_4x^4 + \cdots$ with $a_0, a_2, a_3, a_4, \ldots \in \mathbb{R}$. That is, $\mathbb{R}[x^2, x^3]$ is the set of all polynomials with real-number coefficients and zero linear term. This is an integral domain. (Use the subring test to show that $\mathbb{R}[x^2, x^3]$ is a subring of the ring of polynomials $\mathbb{R}[x]$ with real number coefficients. Because $\mathbb{R}[x]$ is an integral domain, it follows readily that $\mathbb{R}[x^2, x^3]$ is also an integral domain. We will deal with polynomial rings more thoroughly below.) In $\mathbb{R}[x^2, x^3]$ the element x^2 is irreducible, but it is not prime. To see that x^2 is not prime, note that $x^2x^4 = x^6 = x^3x^3$ and so $x^2|x^3x^3$; however, $x^2 \nmid x^3$ because $x \notin \mathbb{R}[x^2, x^3]$.

DEFINITION 7.4. Let R be an integral domain. If every nonzero nonunit of R can be written as a (finite) product of prime elements, then R is a *unique factorization domain* or UFD for short. If every ideal of R is principal, then R is a *principal ideal domain* or PID for short.

EXAMPLE 7.5. $\mathbb{Z}$ is a PID and a UFD. A field k is a PID and a UFD. We will see below that every PID is a UFD, but not every UFD is a PID.

PROPOSITION 7.6. *Let R be an integral domain. Prime factorization in R is unique up to order and multiplication by units: Let $p_1, \dots, p_k, q_1, \dots, q_m$ be primes elements of R such that $p_1 \cdots p_k = q_1 \cdots q_m$, then $m = k$ and there is a permutation $\sigma \in S_k$ and there are units $u_1, \dots, u_k$ in R such that $p_i = u_i q_{\sigma(i)}$ for $i = 1, \dots, k$.*

PROOF. We proceed by induction on k.

Base case: $k = 1$. We need to show $m = 1$, so suppose $m > 1$. Then $p_1 = q_1 \cdots q_m$ and so $p_1 \big| q_i$ for some i because p_1 is prime. Reorder the q_j to assume $p_1 \big| q_1$. Since $q_1 \big| q_1 \cdots q_m = p_1$, we also have $q_1 \big| p_1$. Hence, we have $(q_1) = (p_1) = (q_1 q_2 \cdots q_m)$ and so $q_2 \cdots q_m$ is a unit. This implies that some q_j is a unit, contradicting the fact that q_j is prime.

Induction step. Assuming that $p_1 \cdots p_k = q_1 \cdots q_m$ and $k \geqslant 2$, we have $p_1 \big| p_1 \cdots p_k$ and so $p_1 \big| q_1 \cdots q_m$. Since p_1 is prime, $p_1 \big| q_j$ for some j. As above, reorder the q_i to assume $p_1 \big| q_1$, and use the fact that q_1 is prime to conclude that $p_1 = u_1 q_1$ for some unit u_1. It follows that $p_2 \cdots p_k = u_1^{-1} q_2 \cdots q_m$, so the rest of the result follows by induction. □

PROPOSITION 7.7. *If R is a UFD, then every irreducible element of R is prime.*

PROOF. Fix an irreducible element $x \in R$. Since R is a UFD, we can write $x = p_1 \cdots p_k$ where each $p_i \in R$ is prime. In particular, no p_i is a unit. Suppose $k > 1$. Then $x = p_1(p_2 \cdots p_k)$. Since x is irreducible, either p_1 is a unit or $p_2 \cdots p_k$ is a unit. This contradicts the fact that no p_i is a unit, so we must have $k = 1$. That is $x = p_1$ is prime. □

Here we reconcile our definition of UFD with Hungerford's definition, which is condition (iii).

PROPOSITION 7.8. *Let R be an integral domain. TFAE.*

(i) *R is a UFD;*
(ii) *Every irreducible element of R is prime, and every nonzero nonunit of R can be written as a finite product of irreducible elements;*
(iii) *Every nonzero nonunit of R can be written as a finite product of irreducible elements and such a factorization is unique up to order and multiplication by units.*

PROOF. (ii) $\implies$ (i) Definition of UFD.

(i) $\implies$ (iii) This follows from the definition of UFD and Propositions 7.1 and 7.6.

(iii) $\implies$ (ii) It suffices to show that every irreducible element $x \in R$ is prime. Suppose that $a, b \in R$ and $x \big| ab$. We need to show that $x \big| a$ or $x \big| b$. There is an element $c \in R$ such that $ab = xc$. If $a = 0$, then $a = 0 = x0 \implies x \big| a$. So assume $a \neq 0$, and similarly assume $b \neq 0$. Note that this implies $c \neq 0$.

If a is a unit, then $b = x(a^{-1}c) \implies x\big|b$. So, assume that a is not a unit, and similarly assume that b is not a unit. If c is a unit, then $x = (c^{-1}a)b$; since x is irreducible, either $c^{-1}a$ is a unit or b is a unit. That is, either a is a unit or b is a unit, a contradiction.

Since a, b, c are nonzero nonunits, there are irreducible elements

$$a_1, \dots, a_k, b_1, \dots, b_l, c_1, \dots, c_m \in R$$

such that $a = a_1 \cdots a_k$, $b = b_1 \cdots b_l$ and $c = c_1 \cdots c_m$. The equation $xc = ab$ implies

$$xc_1 \cdots c_m = a_1 \cdots a_k b_1 \cdots b_l.$$

The uniqueness condition for factorizations implies that x is a unit multiple of one of the elements $a_1, \dots, a_k, b_1, \dots, b_l$. If $x = ub_i$, then

$$b = b_1 \cdots b_l = u^{-1}b_1 \cdots b_{i-1}(ub_i)b_{i+1} \cdots b_l = u^{-1}b_1 \cdots b_{i-1}xb_{i+1} \cdots b_l$$

and so $x\big|b$. Similarly, if $x = ua_j$, then $x\big|a$. Hence x is prime. □

8. Day 8

Example 8.1. Factorization into products of irreducibles is not unique if R is not a UFD. For example, in the ring $\mathbb{R}[x^2, x^3]$, the elements x^2, x^3 are irreducible and $x^2x^2x^2 = x^3x^3$. Hence, the number of irreducible factors need not be the same, and the factors need not be unit multiples of each other.

The next lemma says that every PID is noetherian. More on this later.

Lemma 8.2. *Let R be a PID. Given a chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$, there exists an integer $N \geqslant 1$ such that, for every $n \geqslant N$ we have $I_n = I_N$.*

Proof. Each ideal I_j is principal, say $I_j = (a_j)$. As in the proof of Proposition 5.1, since the ideals I_j form a chain, the union $I = \cup_{j \geqslant 1} I_j$ is an ideal of R. Hence $I = (a)$ for some $a \in I = \cup_{j \geqslant 1} I_j$, say $a \in I_N$. For each $n \geqslant N$, we have

$$I_N \subseteq I_n \subseteq I = (a) \subseteq I_N$$

and so $I_n = I_N$. □

We will see below that the converse to the next result fails: If k is a field, then the polynomial ring $k[x, y]$ is a UFD and not a PID.

Theorem 8.3. *Every PID is a UFD.*

Proof. Let R be a PID.

Step 1. Every irreducible element $x \in R$ is prime; moreover, the ideal (x) is maximal. Let I be an ideal such that $(x) \subseteq I \subseteq R$. There is an element $a \in I$ such that $I = (a)$, and so $(x) \subseteq (a)$. By an exercise, this means $a\big|x$, say $x = ab$. Since x is irreducible, either a or b is a unit. If a is a unit, then $I = (a) = R$. If b is a unit, then $I = (a) = (ab) = (x)$. Thus, (x) is maximal. Proposition 5.2(b) implies that (x) is prime, hence x is prime.

Step 2. Every nonzero nonunit $y \in R$ has an irreducible factor. If y is irreducible, then y is an irreducible factor of y and we are done. So, assume y is not irreducible. Then $y = y_1z_1$ where y_1, z_1 are nonzero nonunits. If y_1 is irreducible, then it is an irreducible factor of y and we are done. So, assume y_1 is not irreducible. Then $y_1 = y_2z_2$ where y_2, z_2 are nonzero nonunits. Continue this process, writing $y_n = y_{n+1}z_{n+1}$. Eventually, y_n will be irreducible, as follows.

Suppose $y_n = y_{n+1}z_{n+1}$ for $n = 1, 2, \ldots$ where y_i, z_i are nonzero nonunits for each i. Then $y_{n+1} \big| y_n$ for each n, and so we have

$$(y_1) \subseteq (y_2) \subseteq (y_3) \subseteq \cdots .$$

By Lemma 8.2, we have $(y_N) = (y_{N+1})$ for some $N \geqslant 1$. Since $y_N = y_{N+1}z_{N+1}$, this implies z_{N+1} is a unit, a contradiction.

Step 3. Every nonzero nonunit $z \in R$ can be written as a finite product of irreducible elements. By Step 2, we know that z has an irreducible factor z_1, say $z = z_1w_1$. If w_1 is a unit, then z is irreducible and we are done. So, assume that w_1 is a nonunit, necessarily nonzero because $z \neq 0$. Then w_1 has an irreducible factor z_2, say $w_1 = z_2w_2$. Continuing this process, we see that the argument of Step 2 implies that the process terminates in finitely many steps, yielding a factorization $z = z_1 \cdots z_N$ with each z_i irreducible.

Now apply Proposition 7.8 to conclude that R is a UFD. □

Definition 8.4. An integral domain R is a *Euclidean domain* or ED for short if there exists a function $\varphi\colon R - \{0\} \to \mathbb{N}$ satisfying the following property: for all $a, b \in R$, if $b \neq 0$, then there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$.

Example 8.5. In $\mathbb{Z}$ let $\varphi(n) = |n|$. This is the division algorithm.

Theorem 8.6. *Every ED is a PID.*

Proof. Let R be an ED and fix an ideal $0 \neq I \subseteq R$. We need to find an element $b \in I$ such that $I = (b)$. The set

$$\{\varphi(a) \mid 0 \neq a \in I\}$$

is a nonempty subset of $\mathbb{N}$ and hence has a minimal element. That is, there is an element $0 \neq b \in I$ such that $\varphi(b) \leqslant \varphi(c)$ for all $c \in I$.

Claim: $I = (b)$. Since $b \in I$, we know $I \supseteq (b)$. For the containment $I \subseteq (b)$, fix an element $a \in I$. By assumption, there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$. Notice that $a, bq \in I$ and so $r = a - bq \in I$. If $r \neq 0$, then $\varphi(r) < \varphi(b)$; however, the minimality of $\varphi(b)$ implies $\varphi(r) \geqslant \varphi(b)$, a contradiction. Hence $r = 0$ and so $a = bq \in (b)$. □

Remark 8.7. In summary, we have the following: ED $\overset{(8.6)}{\Longrightarrow}$ PID $\overset{(8.3)}{\Longrightarrow}$ UFD and ED $\overset{\mathbb{Z}[\sqrt{-19}/2]}{\not\Longleftarrow}$ PID $\overset{k[x,y]}{\not\Longleftarrow}$ UFD. We will see below that, if R is a UFD, then the polynomial ring $R[x_1, \ldots, x_n]$ is a UFD. In particular, if k is a field, then $k[x_1, \ldots, x_n]$ is a UFD. However, if $n \geqslant 1$, then $R[x_1, \ldots, x_n]$ is a PID if and only if R is a field and $n = 1$ if and only if $R[x_1, \ldots, x_n]$ is an ED.

Exercise 8.8. Read about GCD's in Hungerford: p. 140. See also Definition 13.1.

Now we formally treat polynomial rings.

Definition 8.9. Let R be a ring. We define the polynomial ring in one indeterminate over R as follows: Let $R[x]$ denote the additive abelian group

$$R^{(\mathbb{N})} = \{(r_0, r_1, r_2, \ldots) \mid r_j \in R \text{ for all } j \geqslant 0 \text{ and } r_j = 0 \text{ for } j \gg 0\}.$$

Hence, addition and subtraction are defined coordinatewise

$$(r_0, r_1, r_2, \ldots) + (s_0, s_1, s_2, \ldots) = (r_0 + s_0, r_1 + s_1, r_2 + s_2, \ldots)$$
$$(r_0, r_1, r_2, \ldots) - (s_0, s_1, s_2, \ldots) = (r_0 - s_0, r_1 - s_1, r_2 - s_2, \ldots)$$
$$0_{R[x]} = (0_R, 0_R, 0_R, \ldots).$$

Define multiplication via the formula

$$(r_0, r_1, r_2, \ldots)(s_0, s_1, s_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

where

$$c_j = \sum_{i=0}^{j} r_i s_{j-i} = \sum_{m+n=j} r_m s_n.$$

Computations:

$$(0, \ldots, 0, r_i, r_{i+1}, r_{i+2}, \ldots, r_d, 0, \ldots)(0, \ldots, 0, s_j, s_{j+1}, s_{j+2}, \ldots, s_e, 0, \ldots)$$
$$= (0, \ldots, 0, r_i s_j, r_i s_{j+1} + r_{i+1} s_j, r_i s_{j+2} + r_{i+1} s_{j+1} + r_{i+2} s_j, \ldots, r_d s_e, 0, \ldots).$$

and

$$(r_0, r_1, r_2, \ldots)(s, 0, 0, \ldots) = (r_0 s, r_1 s, r_2 s, \ldots)$$

9. Day 9

THEOREM 9.1. *Let R be a ring.*

(a) *With the above operations, $R[x]$ is a ring.*
(b) *The function $f\colon R \to R[x]$ given by $f(r) = (r, 0, 0, \ldots)$ is a monomorphism of rings.*
(c) *R is commutative if and only if $R[x]$ is commutative.*
(d) *R has identity if and only if $R[x]$ has identity.*
(e) *R is an integral domain if and only if $R[x]$ is an integral domain.*

PROOF. (a) We already know that $R[x]$ is an additive abelian group, so it remains to show that multiplication is well-defined, associative, and distributive. For well-definedness, we only need to check closure. Fix $(r_0, r_1, r_2, \ldots), (s_0, s_1, s_2, \ldots) \in R[x]$. The element $c_j = \sum_{i=0}^{j} r_i s_{j-i}$ is a finite sum of products of elements of R and, hence, is in R. And the above computation shows that $c_j = 0$ for $j \gg 0$. The proofs of associativity and distributivity are exercises.

(b) By definition, we have

$$f(r + s) = (r + s, 0, 0, \ldots) = (r, 0, 0, \ldots) + (s, 0, 0, \ldots) = f(r) + f(s)$$
$$f(rs) = (rs, 0, 0, \ldots) = (r, 0, 0, \ldots)(s, 0, 0, \ldots) = f(r)f(s).$$

To see that f is a monomorphism: $f(r) = 0$ if and only if $(r, 0, 0, \ldots) = (0, 0, 0, \ldots)$ if and only if $r = 0$.

(c) ($\Longrightarrow$) Assume that R is commutative. Then

$$\sum_{m+n=j} r_m s_n = \sum_{m+n=j} s_m r_n.$$

The left-hand side is the jth entry of the product $(r_0, r_1, r_2, \ldots)(s_0, s_1, s_2, \ldots)$, and the right-hand side is the jth entry of the product $(s_0, s_1, s_2, \ldots)(r_0, r_1, r_2, \ldots)$.

($\Longleftarrow$) Assume that $R[x]$ is commutative. For $r, s \in R$, we have $f(rs) = f(r)f(s) = f(s)f(r) = f(sr)$. Since f is 1-1, this implies $rs = sr$.

(d) ($\Longrightarrow$) Assume that R has identity 1. Then $(1, 0, 0, \ldots)$ is a multiplicative identity for $R[x]$:

$$(1, 0, 0, \ldots)(r_0, r_1, r_2, \ldots) = (1r_0, 1r_1, 1r_2, \ldots) = (r_0, r_1, r_2, \ldots)$$

and similarly for $(r_0, r_1, r_2, \ldots)(1, 0, 0, \ldots)$.

($\Longleftarrow$) Assume that $R[x]$ has identity $(e_0, e_1, e_2, \ldots)$. It follows that, for all $r \in R$, we have

$$(r, 0, 0, \ldots) = (r, 0, 0, \ldots)(e_0, e_1, e_2, \ldots) = (re_0, re_1, re_2, \ldots)$$

and so $re_0 = r$. Similarly, we have $e_0 r = r$ and so e_0 is a multiplicative identity for R.

(e) ($\Longrightarrow$) Assume that R is an integral domain. Then R is a nonzero commutative ring with identity, and so the same is true of $R[x]$. Fix elements $0 \neq (r_0, r_1, r_2, \ldots), (s_0, s_1, s_2, \ldots) \in R$. Then there exist $i, j \geqslant 0$ such that $r_i \neq 0$ and $r_m = 0$ for all $m < i$ and $s_j \neq 0$ and $s_n = 0$ for all $n < j$. Then, we have $r_i s_j \neq 0$ and so

$$\begin{aligned}
&(r_0, r_1, r_2, \ldots)(s_0, s_1, s_2, \ldots) \\
&\quad = (0, \ldots, 0, r_i, r_{i+1}, r_{i+2}, \ldots)(0, \ldots, 0, s_j, s_{j+1}, s_{j+2}, \ldots) \\
&\quad = (0, \ldots, 0, r_i s_j, r_i s_{j+1} + r_{i+1} s_j, r_i s_{j+2} + r_{i+1} s_{j+1} + r_{i+2} s_j, \ldots, r_d s_e, 0, \ldots) \\
&\quad \neq 0
\end{aligned}$$

($\Longleftarrow$) Assume that $R[x]$ is an integral domain. Then $R[x]$ is a nonzero commutative ring with identity, and so the same is true of R. Suppose $0 \neq r, s \in R$. Then $f(r), f(s) \neq 0$ and so

$$f(rs) = f(r) f(s) \neq 0$$

and so $rs \neq 0$. □

Remark 9.2. We frequently identify R with its image in $R[x]$. This yields formulas like:

$$r(r_0, r_1, r_2, \ldots) = (rr_0, rr_1, rr_2, \ldots).$$

Here is a more familiar presentation:

Proposition 9.3. *Let R be a ring with identity and set $x = (0, 1, 0, 0, \ldots)$ in $R[x]$.*

(a) *For each $n \geqslant 1$, we have $x^n = (\underbrace{0, 0, \ldots, 0}_{n}, 1, 0, 0, \ldots)$.*

(b) *For each $r \in R$ and each $n \geqslant 1$, we have*

$$rx^n = (\underbrace{0, 0, \ldots, 0}_{n}, r, 0, 0, \ldots) = x^n r.$$

(c) *For each $f \in R[x]$ there is an integer $d \geqslant 0$ and elements $r_0, r_1, \ldots, r_d \in R$ such that*

$$f = \textstyle\sum_{i=0}^{d} r_i x^i = r_0 + r_1 x + r_2 x^2 + \cdots + r_d x^d.$$

Proof. (a) Exercise. By induction on n.

(b) From part (a).

(c) We have

$$\begin{aligned}
f &= (r_0, r_1, r_2, \ldots, r_d, 0, 0, \ldots) \\
&= r_0(1, 0, 0, \ldots) + r_1(0, 1, 0, \ldots) + \cdots + r_d(0, 0, \ldots, 0, 1, 0, \ldots) \\
&= r_0 + r_1 x + r_2 x^2 + \cdots + r_d x^d.
\end{aligned}$$

□

DEFINITION 9.4. Let R be a ring. The polynomial ring in two indeterminates over R is the ring

$$R[x,y] = R[x][y] \qquad \text{or} \qquad R[x_1,x_2] = R[x_1][x_2].$$

Inductively, the polynomial ring in n indeterminates over R is the ring

$$R[x_1,\dots,x_n] = R[x_1,\dots,x_{n-1}][x_n].$$

The next result follows from the previous ones using induction on n. See also Hungerford pp. 151-152.

PROPOSITION 9.5. *Let R be a ring and $n \geqslant 1$.*

(a) *$R[x_1,\dots,x_n]$ is a ring.*
(b) *Assume that R has identity. Let $f \in R[x_1,\dots,x_n]$. For each element $\mathbf{a} = (a_1,\dots,a_n) \in \mathbb{N}^n$ there is an element $r_{\mathbf{a}} \in R$ such that $r_{\mathbf{a}} = 0$ for all but finitely many $\mathbf{a} \in \mathbb{N}^n$ and*
$$f = \textstyle\sum_{\mathbf{a}\in\mathbb{N}^n} r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}.$$
(c) *Assume that R has identity. The function $f\colon R \to R[x_1,\dots,x_n]$ given by $f(r) = rx_1^0 \cdots x_n^0$ is a monomorphism of rings.*
(d) *R is commutative if and only if $R[x_1,\dots,x_n]$ is commutative.*
(e) *R has identity if and only if $R[x_1,\dots,x_n]$ has identity.*
(f) *R is an integral domain if and only if $R[x_1,\dots,x_n]$ is an integral domain.*
(g) *For each k such that $1 < k < n$, there is an isomorphism $R[x_1,\dots,x_n] \cong R[x_1,\dots,x_k][x_{k+1},\dots,x_n]$.*
(h) *For each $\sigma \in S_n$ there is an isomorphism $R[x_1,\dots,x_n] \cong R[x_{\sigma(1)},\dots,x_{\sigma(n)}]$.*
(i) *Assume that R has identity. For all $r,s \in R$ and all $a_1,\dots,a_n,b_1,\dots,b_n \in \mathbb{N}$, we have*
$$(rx_1^{a_1}\cdots x_n^{a_n})(sx_1^{b_1}\cdots x_n^{b_n}) = rsx_1^{a_1+b_1}\cdots x_n^{a_n+b_n}.$$

□

10. Day 10

DEFINITION 10.1. If S is a ring, then the *center* of S is

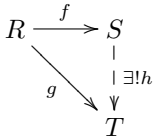
$$Z(S) = \{s \in S \mid ss' = s's \text{ for all } s' \in S\}.$$

Using the subring test, we see that the center $Z(S)$ is a subring of S.

Let R be a commutative ring with identity. For each $r \in R$, set $r^0 = 1$.

An *R-algebra* is a ring S with identity equipped with a homomorphism of rings with identity $f\colon R \to S$ such that $\mathrm{Im}(f) \subseteq Z(S)$.

Let S and T be R-algebras via the maps $f\colon R \to S$ and $g\colon R \to T$. A *homomorphism of R-algebras* from S to T is a ring homomorphism $h\colon S \to T$ making the following diagram commute.



Note that, because $f(1) = 1$ and $g(1) = 1$, we have $h(1) = 1$.

EXAMPLE 10.2. Let R be a commutative ring with identity.

R is an R-algebra via the identity map $R \to R$.

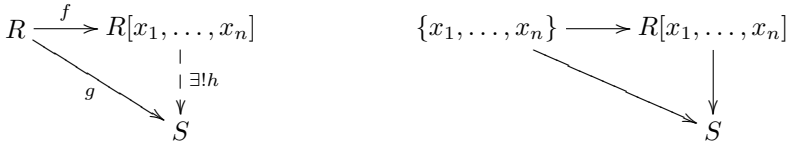
The polynomial ring $R[x_1, \ldots, x_n]$ is an R-algebra via the natural map $R \to R[x_1, \ldots, x_n]$.

The ring $M_n(R)$ of $n \times n$ matrices with entries from R is an R-algebra via the map $R \to M_n(R)$ given by

$$r \mapsto rI_n = \begin{pmatrix} r & 0 & \cdots & 0 \\ 0 & r & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r \end{pmatrix}.$$

Here is the universal property for polynomial rings. It includes the prototype for R-algebra homomorphisms. The maps h are often called evaluation homomorphisms: they are given by $P(x_1, \ldots, x_n) \mapsto P(s_1, \ldots, s_n)$.

PROPOSITION 10.3. *Let R be a commutative ring with identity, and let $f\colon R \to R[x_1, \ldots, x_n]$ be the natural map. Let S be an R-algebra via the homomorphism $g\colon R \to S$. For each list $s_1, \ldots, s_n \in Z(S)$ there exists a unique homomorphism of R-algebras $h\colon R[x_1, \ldots, x_n] \to S$ such that $h(x_i) = s_i$ for each i. In particular, the following diagrams commute*



and S is an $R[x_1, \ldots, x_n]$-algebra.

PROOF. Define h by the following formula:

$$h\left(\textstyle\sum_{\mathbf{a} \in \mathbb{N}^n} r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}\right) = \sum_{\mathbf{a} \in \mathbb{N}^n} g(r_{\mathbf{a}}) s_1^{a_1} \cdots s_n^{a_n}$$

where $\mathbf{a} = (a_1, \ldots, a_n)$. The uniqueness of representation of polynomials shows that this is well-defined. It is routine to check that h is a ring homomorphism with the desired properties. For instance, the first diagram commutes because

$$h(f(r)) = h(rx_1^0 \cdots x_n^0) = g(r)s_1^0 \cdots s_n^0 = g(r)1_s = g(r).$$

For the uniqueness of h, suppose that $H\colon R[x_1, \ldots, x_n] \to S$ is another homomorphism of R-algebras such that $H(x_i) = s_i$ for each i. For each $\mathbf{a} \in \mathbb{N}^n$ and each $r_{\mathbf{a}} \in R$, we then have

$$H(r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}) = H(f(r_{\mathbf{a}}))H(x_1)^{a_1} \cdots H(x_n)^{a_n} = g(r_{\mathbf{a}}) s_1^{a_1} \cdots s_n^{a_n} = h(r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}).$$

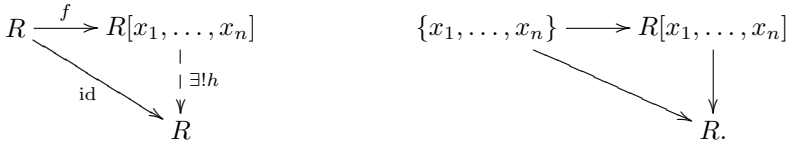
Since H preserves finite sums, it follows that

$$h\left(\textstyle\sum_{\mathbf{a} \in \mathbb{N}^n} r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}\right) = \sum_{\mathbf{a} \in \mathbb{N}^n} g(r_{\mathbf{a}}) s_1^{a_1} \cdots s_n^{a_n} = H\left(\textstyle\sum_{\mathbf{a} \in \mathbb{N}^n} r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}\right)$$

and so $H = h$. □

COROLLARY 10.4. *Let R be a commutative ring with identity, and let $f\colon R \to R[x_1, \ldots, x_n]$ be the natural map. For each list $r_1, \ldots, r_n \in R$ there exists a unique homomorphism of R-algebras $h\colon R[x_1, \ldots, x_n] \to r$ such that $h(x_i) = r_i$ for each i.*

In particular, the following diagrams commute:



Given a polynomial $P = P(x_1, \ldots, x_n)$ we write $h(P) = P(r_1, \ldots, r_n)$. □

PROPOSITION 10.5. *Let R be a commutative ring with identity and let $0 \neq f, g \in R[x]$.*

(a) *If $fg \neq 0$, then $\deg(fg) \leqslant \deg(f) + \deg(g)$.*
(b) *If the leading coefficient of f is not a zero-divisor (e.g., if the leading coefficient of f is a unit or if R is an integral domain), then $\deg(fg) = \deg(f) + \deg(g)$.*
(c) *If $f + g \neq 0$, then $\deg(f + g) \leqslant \max\{\deg(f), \deg(g)\}$.*
(d) *If $\deg(f) \neq \deg(g)$, then $f + g \neq 0$ and $\deg(f + g) = \max\{\deg(f), \deg(g)\}$.*

PROOF. (a) and (b). Let $d = \deg(f)$ and $e = \deg(g)$. The computation of Definition 8.9 shows that $\deg(fg) \leqslant d + e = \deg(f) + \deg(g)$. Furthermore, the coefficient of x^{d+e} in fg is the product of the leading coefficients of f and g. So, equality holds if the product of the leading coefficients of f and g is nonzero.

(c) and (d) follow from similar computations. □

Here is the division algorithm for polynomial rings. As with the division algorithm in $\mathbb{Z}$, this is the key to all the factorization properties in $R[x]$.

THEOREM 10.6. *Let R be a commutative ring with identity, and fix a polynomial $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ such that a_n is a unit in R. For each polynomial $g \in R[x]$ there exist unique $q, r \in R[x]$ such that $g = qf + r$ and either $r = 0$ or $\deg(r) < \deg(f)$.*

PROOF. First, we deal with existence.

Because a_n is a unit in R, we may assume without loss of generality that $a_n = 1$. We may also assume without loss of generality that f is not a constant polynomial. In particular, we have $\deg(f) \geqslant 1$.

If $g = 0$ or $\deg(g) < \deg(f)$, then the polynomials $q = 0$ and $r = g$ satisfy the desired conclusions.

We assume that $g \neq 0$ and proceed by induction on $d = \deg(g)$. The base case $d = 0$ follows from the previous paragraph, as do the cases $d < \deg(f)$. Therefore, assume that $d \geqslant \deg(f)$ and that the result holds for all polynomials $h \in R[x]$ such that $\deg(h) < d$. Let b_d be the leading coefficient of g. Then the polynomial $h = g - b_d x^{d-n} f$ is either 0 or has $\deg(h) < d$. Hence, the induction hypothesis provides polynomials $q_1, r \in R[x]$ such that

$$q_1 f + r = h = g - b_d x^{d-n} f$$

and either $r = 0$ or $\deg(r) < \deg(f)$. It follows that

$$g = [q_1 + b_d x^{d-n}] f + r$$

so the polynomials $q = q_1 + b_d x^{d-n}$ and r satisfy the desired properties.

Now for uniqueness. Assume $qf + r = g = q_2 f + r_2$ where (1) either $r = 0$ or $\deg(r) < \deg(f)$, and (2) either $r_2 = 0$ or $\deg(r_2) < \deg(f)$. Then $r - r_2 = (q_2 - q)f$.

The leading coefficient of f is a unit. If $q \neq q_2$, then $r - r_2 = (q_2 - q)f \neq 0$. In particular, either $r \neq 0$ or $r_2 \neq 0$. If $r, r_2 \neq 0$, then Proposition 10.5 implies

$$\begin{aligned}\deg(f) &\leqslant \deg(f) + \deg(q_2 - q) = \deg((q_2 - q)f) \\ &= \deg(r - r_2) \leqslant \max\{\deg(r), \deg(r_2)\} < \deg(f)\end{aligned}$$

a contradiction. The cases where $r = 0$ or $r_2 = 0$ similarly yield contradictions. Thus, we have $q = q_2$ and $r - r_2 = (q_2 - q)f = 0$ and so $r = r_2$. □

COROLLARY 10.7 (Remainder Theorem). *Let R be a commutative ring with identity, and fix $s \in R$. For each polynomial $g \in R[x]$ there exist unique $q \in R[x]$ such that $g = q \cdot (x - r) + g(s)$.*

PROOF. Apply the division algorithm. It suffices to show that $r = g(s)$. Because either $r = 0$ or $\deg(r) < \deg(x - s) = 1$, we know that r is constant. The evaluation homomorphism yields

$$g(s) = q(s)(s - s) + r(s) = 0 + r = r$$

as desired. □

11. Day 11

DEFINITION 11.1. Let R be a commutative ring with identity and $P \in R[x]$. An element $r \in R$ is a *root* of P if $P(r) = 0$.

PROPOSITION 11.2. *Let S be an integral domain and $R \subseteq S$ a nonzero subring such that R has identity.*

(a) *Then R is an integral domain and $1_S = 1_R$.*
(b) *If $0 \neq f \in R[x]$ and $\deg(f) = n$, then f has at most n roots in S; in particular, f has at most n roots in R.*

The conclusions in this result fail if S is not an integral domain.

PROOF. (a) It is straightforward to show that R is an integral domain. To see that $1_R = 1_S$, note that $1_S 1_R = 1_R = 1_R 1_R$, so that cancellation implies $1_S = 1_R$.

(b) Proceed by induction on $n = \deg(f)$. If $n = 0$, then f is a nonzero constant and therefore has no roots.

Inductively, assume that the result holds for polynomials of degree $< n$. If f has no roots in S, then we are done. So assume that $s \in S$ is a root of f. The Remainder Theorem implies that there is a unique $q \in S[x]$ such that $f = (x - s)q$. By Proposition 10.5(b) we have $\deg(q) = \deg(f) - 1 = n - 1 < n$, and so the induction hypothesis implies that q has at most $n - 1$ roots in S.

Let $t \in S$ be a root of f. Since the map $S[x] \to S$ given by $P \mapsto P(t)$ is a ring homomorphism, it implies that $0 = f(t) = (t - s)q(t)$. Since S is an integral domain, either $t - s = 0$ or $q(t) = 0$. That is, either $t = s$ or t is a root of q. Since q has at most $n - 1$ roots, this implies that f has at most n roots. □

EXAMPLE 11.3. Let $R = \mathbb{R}[x]/(x^2)$ and set $\overline{x} = x + (x^2) \in R$. Then the polynomial $y^2 \in R[y]$ has infinitely many roots, namely, every element of the form $\lambda\overline{x}$ for some $\lambda \in \mathbb{R}$.

REMARK 11.4. Here is a word of warning. Let $P \in \mathbb{R}[x]$. From calculus/college algebra we know that $P = 0$ if and only if $P(r) = 0$ for all $r \in \mathbb{R}$. This can fail if $\mathbb{R}$ is replaced with an arbitrary ring R, even when R is a field.

For example, let p be a positive prime integer and set $R = \mathbb{Z}/p\mathbb{Z}$. It is a fact that, for each $\overline{n} \in R$, we have $\overline{n}^p = \overline{n}$. (This is called Fermat's Little Theorem; see Corollary 11.8.) In particular, every element of R is a root of the polynomial $x^p - x$, even though this polynomial is nonzero. This shows the importance of distinguishing between the polynomial P and the function $R \to R$ given by evaluating the polynomial P.

Note, however, that this is only a problem with finite fields as the following can by shown relatively easily using Proposition 11.2(b): If k is an *infinte* field and $P \in k[x]$ has infinitely many roots in k, then $P = 0$.

REMARK 11.5. Let R be a commutative ring with identity and set $R^\times = \{\text{units in } R\}$. It is straightforward to show that $R^\times$ is an abelian group under multiplication. In particular, if k is a field, then $k^\times = k - \{0\}$.

PROPOSITION 11.6. *Let k be a field. Then any finite subgroup $G \leqslant k^\times$ is cyclic.*

PROOF. Assume $G \neq \{1\}$. Then G is a finite abelian group, so the fundamental theorem of finitely generated abelian groups implies that there exist (not necessarily distinct) prime integers $p_1, \dots, p_r \geqslant 2$ and positive integers $a_1, \dots, a_r$ such that $G \cong \oplus_{i=1}^r \mathbb{Z}/p_i^{a_i}\mathbb{Z}$.

Note that G is written multiplicatively and the $\mathbb{Z}/p_i^{a_i}\mathbb{Z}$ are written additively. Identify each $\mathbb{Z}/p_i^{a_i}\mathbb{Z}$ with a subgroup of $\oplus_{i=1}^r \mathbb{Z}/p_i^{a_i}\mathbb{Z}$ in the natural way. Note that, under this identification, we have $\mathbb{Z}/p_i^{a_i}\mathbb{Z} \cap \mathbb{Z}/p_j^{a_j}\mathbb{Z} = \{0\}$ when $i \neq j$. There are p_i distinct elements $\overline{n} \in \mathbb{Z}/p_i^{a_i}\mathbb{Z}$ such that $p_i\overline{n} = 0$, namely $\overline{p_i^{a_i-1}}, \overline{2p_i^{a_i-1}}, \dots, \overline{p_i p_i^{a_i-1}} = \overline{0}$. Thus, there are p_i elements $g \in G$ such that $g^{p_i} = 1$.

Suppose that $p_i = p_j$ for some $i \neq j$. The previous paragraph shows that there are at least $2p_i - 1 > p_i$ elements $g \in G$ such that $g^{p_i} = 1$. This shows that the polynomial $x^{p_i} - 1 \in k[x]$ has more than p_i roots, contradicting Proposition 11.2(b).

Thus, we have $\gcd(p_i, p_j) = 1$ for all $i \neq j$, and it follows that

$$G \cong \oplus_{i=1}^r \mathbb{Z}/p_i^{a_i}\mathbb{Z} \cong \mathbb{Z}/(p_1^{a_1} \cdots p_r^{a_r})\mathbb{Z}.$$

That is G is cyclic. □

COROLLARY 11.7. *If p is a positive prime integer, then $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.*

PROOF. The group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic and has exactly $p - 1$ elements. □

COROLLARY 11.8 (Fermat's Little Theorem). *Let p be a positive prime integer.*

(a) *For each $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$, we have $\overline{n}^p = \overline{n}$.*
(b) *In $\mathbb{Z}/p\mathbb{Z}[x]$ we have $\prod_{\overline{n} \in \mathbb{Z}/p\mathbb{Z}}(x - \overline{n}) = x^p - x$.*

PROOF. (a) The case where $\overline{n} = \overline{0}$ is easy. For the remaining cases, use the isomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$: Since $(p-1)(n + (p-1)\mathbb{Z}) = 0 + (p-1)\mathbb{Z}$, this translates to $\overline{n}^{p-1} = \overline{1}$ for all $\overline{n} \neq \overline{0}$ in $\mathbb{Z}/p\mathbb{Z}$, and so $\overline{n}^p = \overline{n}$.

(b) From part (a) we know that each element of $\mathbb{Z}/p\mathbb{Z}$ is a root of the polynomial $x^p - x \in \mathbb{Z}/p\mathbb{Z}[x]$. Repeatedly apply the Remainder Theorem to write

$$x^p - x = q \prod_{\overline{n} \in \mathbb{Z}/p\mathbb{Z}}(x - \overline{n})$$

for some $q \in \mathbb{Z}/p\mathbb{Z}[x]$. Proposition 11.2(b) shows that $\deg(q) = 0$, and so q is a constant. Multiplying out, we see that the product is monic, as q times the product, and so we have $q = 1$. □

DEFINITION 11.9. Let R be an integral domain. For each positive integer n and each $r \in R$, recall that $nr = \underbrace{r + \cdots + r}_{n}$.

For a polynomial $f = \sum_{i=0}^{d} r_i x^i \in R[x]$ define the *formal derivative* of f to be the polynomial

$$f' = \sum_{i=1}^{d} i r_i x^{i-1} = r_1 + 2r_2 x + 3r_3 x^2 + \cdots + d r_d x^{d-1}.$$

The derivative is "formal" because no limits were involved.

REMARK 11.10. Let R be an integral domain. It is straightforward to show that formal differentiation satisfies the following properties: for all $r \in R$ and all $f, g \in R[x]$ and all $n \geqslant 0$, we have

$$(rf)' = rf' \qquad (f+g)' = f' + g'$$
$$(fg)' = f'g + fg' \qquad (f^n)' = nf^{n-1}f'$$

REMARK 11.11. Let R be a commutative ring with identity. Let $r \in R$ and $f \in R[x]$ with $d = \deg(f)$. From the Remainder Theorem we see that r is a root of f if and only if $(x - r) \big| f$, that is, if and only if there exists a polynomial $q \in R[x]$ such that $f = (x - r)q$.

Assume that R is an integral domain and that r is a root of f. Hence the Remainder Theorem implies that there exists a polynomial $q \in R[x]$ such that $f = (x - r)q$. Proposition 11.2(b) implies $\deg(q) = \deg(f) - 1$. This shows that $(x - r)^{d+1} \nmid f$, and so there exists an integer $e \geqslant 1$ such that $(x - r)^e \big| f$ and $(x - r)^{e+1} \nmid f$. The integer e is called the *multiplicity* of the root r of f. We say that r is a *simple root* of f if $e = 1$; otherwise f is a *multiple root* of f.

Note that the above argument shows that $e \leqslant d$. Furthermore, the argument of Proposition 11.2(b) shows the following: if R is a subring of an integral domain S, then f has at most d roots in S counted with multiplicity. In other words, if $s_1, \ldots, s_n \in S$ are the distinct roots of f in S and e_i is the multiplicity of the root s_i of f, then $d \geqslant \sum_i e_i$.

PROPOSITION 11.12. *Let R and S be integral domains such that R is a subring of S, and let $s \in S$. Then s is a multiple root of f if and only if $f(s) = 0 = f'(s)$.*

PROOF. Assume that s is a root of f. It suffices to show that s is a multiple root of f if and only if $f'(s) = 0$. Since s is a root of f, the Remainder Theorem allows us to write $f = (x - s)q$ for some $q \in S[x]$. (Notice that we are implicitly using the fact that $R[x]$ is a subring of $S[x]$.) The product rule for formal derivatives implies

$$f' = [(x - s)q]' = q + (x - s)q'$$

and so $f'(s) = q(s)$. Thus, $f'(s) = 0$ if and only if $q(s) = 0$; this is so if and only if $(x - s) \big| q$ which is so if and only if $(x - s)^2 \big| f$ because $f = (x - s)q$. The last "iff" uses the fact that S is an integral domain. □

DEFINITION 11.13. Let K be a field. A *subfield* of K is a subring $k \subseteq K$ such that k is a field under the operations from K. When k is a subfield of K, we also say that K is a *field extension* of k.

EXAMPLE 11.14. $\mathbb{C}$ is a field extension of $\mathbb{R}$, and $\mathbb{R}$ is a field extension of $\mathbb{Q}$.

Now we construct the field of quotients of an integral domain. It is modeled on the construction of $\mathbb{Q}$ from $\mathbb{Z}$. The elements of $\mathbb{Q}$ are of the form r/s where $r, s \in \mathbb{Z}$ and $s \neq 0$.

CONSTRUCTION 11.15. Let R be an integral domain and consider the Cartesian product $R \times (R - \{0\})$. Define a relation on $R \times (R - \{0\})$ as follows: $(r, s) \sim (r', s')$ if and only if $rs' = r's$. This is an equivalence relation on $R \times (R - \{0\})$, and the set of equivalence classes is denoted $\mathrm{Q}(R)$. The equivalence class of an element (r, s) in $\mathrm{Q}(R)$ is denoted r/s or $\frac{r}{s}$. If $0 \neq t \in R$, then the definition implies $(r, s) \sim (rt, st)$; this translates to the cancellation formula $\frac{rt}{st} = \frac{r}{s}$.

For elements $r/s, t/u \in \mathrm{Q}(R)$, set

$$\frac{r}{s} + \frac{t}{u} = \frac{ru + ts}{su} \qquad \text{and} \qquad \frac{r}{s}\frac{t}{u} = \frac{rt}{su}.$$

PROPOSITION 11.16. *With notation as in Construction 11.15:*

(a) *In* $\mathrm{Q}(R)$*, we have* $r/s = 0/t$ *if and only if* $r = 0$*.*
(b) *In* $\mathrm{Q}(R)$*, we have* $r/s = t/t$ *if and only if* $r = s$*.*
(c) $\mathrm{Q}(R)$ *is a field with* $0_{\mathrm{Q}(R)} = 0_R/1_R$ *and* $1_{\mathrm{Q}(R)} = 1_R/1_R = r/r$ *and* $(r/s)^{-1} = s/r$*.*
(d) *The assignment* $f\colon R \to \mathrm{Q}(R)$ *given by* $r \mapsto r/1$ *is a monomorphism of rings with identity.*

PROOF. (a) $r/s = 0/t$ if and only if $rt = s0$ if and only if $r = 0$; the last equivalence is from the fact that R is an integral domain.

(b) $r/s = t/t$ if and only if $rt = st$ if and only if $r = s$; the last equivalence is by cancellation.

(c) The main point is to show that the addition and multiplication on $\mathrm{Q}(R)$ are well-defined; the other field-axioms are then easily verified. Assume that $r/s = r'/s'$ and $t/u = t'/u'$, that is, $rs' = r's$ and $tu' = t'u$. Then

$$\begin{aligned}\frac{ru + ts}{su} &= \frac{(ru + ts)s'u'}{(su)s'u'} = \frac{rs'uu' + tu'ss'}{ss'uu'} = \frac{r'suu' + t'uss'}{ss'uu'} \\ &= \frac{(r'u' + t's)us}{(u's')us} = \frac{r'u' + t's}{u's'}\end{aligned}$$

so addition is well-defined. The equality $\frac{rt}{su} = \frac{r't'}{s'u'}$ is even easier to verify, showing that multiplication is well-defined.

We have the correct additive identity because

$$\frac{r}{s} + \frac{0}{1} = \frac{r1 + s0}{s1} = \frac{r}{s}$$

and the multiplicative identity is even easier. The other axioms showing that $\mathrm{Q}(R)$ is a commutative ring with identity are straightforward but tedious.

To see that $\mathrm{Q}(R)$ is nonzero, we need to show $0/1 \neq 1/1$: this follows from parts (a) and (c).

Finally, if $r/s \neq 0/1$ then $r \neq 0$ and so $s/r \in \mathrm{Q}(R)$. It is straightforward to check that $\frac{r}{s}\frac{s}{r} = \frac{1}{1}$, and so $(r/s)^{-1} = s/r$.

(d) The function is well-defined. It is straightforward to show that it is a homomorphism of rings with identity: for instance

$$\frac{r}{1}+\frac{r'}{1}=\frac{r1+1r'}{1\cdot 1}=\frac{r+r'}{1}.$$

The fact that f is a monomorphism, follows from part (a). □

We generally identify R with its image in $\mathrm{Q}(R)$.

EXAMPLE 11.17. $\mathrm{Q}(\mathbb{Z})\cong\mathbb{Q}$.

If k is a field and we set $k(x_1,\dots,x_n)=\mathrm{Q}(k[x_1,\dots,x_n])$, then $k(x_1,\dots,x_n)$ is a field extension of k. More generally, if k is a field and R is an integral domain containing k as a subring, then $\mathrm{Q}(R)$ is a field extension of k.

We will see more field extension constructions later.

DEFINITION 11.18. Let R be a commutative ring with identity. An element $r\in R$ is *nilpotent* if $r^n=0$ for some $n\geqslant 1$. An element $s\in R$ is a *zerodivisor* if there exists $0\neq t\in R$ such that $st=0$.

EXAMPLE 11.19. If $r\in R$ is nilpotent, then r is a zerodivisor.

In $\mathbb{Z}/8\mathbb{Z}$, the element $\overline{2}$ is nilpotent.

In $\mathbb{Z}/6\mathbb{Z}$, the element $\overline{2}$ is a zerodivisor. Note that $\mathbb{Z}/6\mathbb{Z}$ has no nonzero nilpotent elements, so not every zerodivisor is nilpotent.

An R is an integral domain if and only if the only zerodivisor in R is 0. In particular, the only nilpotent element element of an integral domain is 0.

12. Day 12

EXERCISE 12.1. Let R be a commutative ring with identity, and let $f=a_0+a_1x+\cdots+a_dx^nd\in R[x]$.

(a) Show that f is nilpotent if and only if each a_i is nilpotent.
(b) Show that f is a unit in $R[x]$ if and only if a_0 is a unit and $a_1,\dots,a_d$ are nilpotent. In particular, if k is a field, then the units of $k[x]$ are precisely the nonzero constant polynomials.
(c) Show that f is a zerodivisor in $R[x]$ if and only if there exists an element $0\neq r\in R$ such that $ra_i{=}0$ for each i. for polynomials in n variables.

THEOREM 12.2. *Let k be a field and $L\supseteq k$ a field extension. Let $f\in k[x]$, and assume that f is irreducible in $k[x]$. If f has a multiple root in L, then $f'=0$.*

PROOF. Let $a\in L$ be a multiple root of f, and suppose $f'\neq 0$. Proposition 11.12 implies $f(a)=0=f'(a)$. Notice that $\deg(f')<\deg(f)$.

Claim: f' and f have no common factors in $R[x]$, other than the units. To see this, suppose that $g\big|f'$ and $g\big|f$. Since $g\big|f'$, we have $\deg(g)\leqslant\deg(f')<\deg(f)$. Since $g\big|f$, we have $f=gh$. Because f is irreducible, either g is a unit or h is a unit. If h were a unit, then it would be constant, that is $\deg(h)=0$ and so $\deg(g)=\deg(f)$, a contradiction. Hence, g is a unit.

Since $k[x]$ is a PID and f,f' have no nontrivial common factors, we see that $(f,f')=(1)$. Hence, there are $P,Q\in R[x]$ such that $1=Pf+Qf'$. Then $1=P(a)f(a)+Q(a)f'(a)=0$, a contradiction. Hence, $f'=0$. □

EXAMPLE 12.3. If $f\in\mathbb{Q}[x]$ is irreducible, then f has no multiple roots in $\mathbb{C}$.

DEFINITION 12.4. Let R be a UFD and $0 \neq f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$. A *content* of f is a greatest common divisor of $\{a_0, a_1, \ldots, a_d\}$ in R. The polynomial f is *primitive* if 1 is a content for f, that is, if the coefficients of f are relatively prime.

REMARK 12.5. Let R be a UFD and $0 \neq f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$.

Recall that greatest common divisors are not uniquely defined. Specifically, if r and s are greatest common divisors of $\{a_0, a_1, \ldots, a_d\}$ in R, then there is a unit $u \in R$ such that $s = ur$. Conversely, if r is a greatest common divisor of $\{a_0, a_1, \ldots, a_d\}$ in R and $u \in R$ is a unit, then ur is a greatest common divisor of $\{a_0, a_1, \ldots, a_d\}$ in R.

We say that $r, s \in R$ are *associates* if there is a unit $u \in R$ such that $s = ur$. Write $r \approx s$ when r and s are associates in R. The relation $\approx$ is an equivalence relation, and the equivalence class of r under this relation is denoted $[r]$. By definition, $[r]$ is the set of all unit multiples of r in R. Note that $[r] = [1]$ if and only if r is a unit in R.

If r, s are contents of f, then the above discussion implies $[r] = [s]$, and we write $C(f) = [r]$. (This notation is not standard. However, most books write $C(f) = r$ or $C(f) \approx r$, which is not well defined.) Conversely, if r is a content for f and $[r] = [s]$, then s is a content for f. Also, if f is constant $f = a_0$, then $C(f) = [a_0]$.

If $r \approx r_1$ and $s \approx s_1$, then $rs \approx r_1s_1$. Hence, the assignment $[r][s] = [rs]$ is well-defined.

EXERCISE 12.6. Let R be a UFD and $0 \neq f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$.

(a) Show that $C(tf) = [t]C(f)$ for each $t \in R$.
(b) Show that, if $C(f) = [r]$, then there is a primitive polynomial g such that $f = rg$.

The following few results are due to Gauss.

LEMMA 12.7. *Let R be a UFD and let $0 \neq f, g \in R[x]$.*

(a) *If f and g are primitive, then so is fg.*
(b) *$C(fg) = C(f)C(g)$.*

PROOF. (a) Assume that f and g are primitive and let $C(fg) = [r]$. We want $[r] = [1]$, that is, we want to show that r is a unit. Note that $r \neq 0$: since R is an integral domain, so is $R[s]$ and so $fg \neq 0$.

Suppose that r is not a unit. Since R is a UFD, this implies that r has a prime factor p. The function $\tau\colon R[x] \to (R/(p))[x]$ given by $\tau(\sum_i a_ix^i) = \sum_i \overline{a_i}x^i$ is a well-defined epimorphism of rings with identity. Check this using the universal property for polynomial rings with the following diagram as your guide:

$$\begin{array}{ccc} R & \longrightarrow & R[x] \\ \downarrow & & \downarrow \tau \\ R/(p) & \longrightarrow & (R/(p))[x]. \end{array}$$

Since $p \mid r$ and $C(fg) = [r]$, we see that p divides each coefficient of fg and so $\tau(fg) = 0$. On the other hand, since f is primitive, we know that p does not divide at least one coefficient of f, and so $\tau(f) \neq 0$. Similarly, we have $\tau(g) \neq 0$. Since p is prime, the ring $R/(p)$ is an integral domain, and hence so is $(R/(p))[x]$. It follows that $0 \neq \tau(f)\tau(g) = \tau(fg)$, a contradiction.

(b) Write $C(f) = [r]$ and $C(g) = [s]$. Use Exercise 12.6(b) to find primitive polynomials $f_1, g_1 \in R[x]$ such that $f = rf_1$ and $g = sg_1$. Note that part (a) implies $C(f_1g_1) = [1]$. This explains the third equality in the next sequence:

$$C(fg) = C((rs)(f_1g_1)) = [rs]C(f_1g_1) = [rs] = [r][s] = C(f)C(g).$$

The first equality is by our choice of f_1 and g_1; the second equality is by Exercise 12.6(a); the remaining equalities are by definition. □

LEMMA 12.8. *Let R be a UFD and let $0 \neq f, g \in R[x]$ and $0 \neq r \in R$.*

(a) *fg is primitive if and only if f and g are primitive.*
(b) *rf is primitive if and only if f is primitive and r is a unit.*
(c) *If f is irreducible in $R[x]$, then f is either constant or primitive.*

PROOF. (a) ($\Longleftarrow$) Lemma 12.7(a).
($\Longrightarrow$) Assume that fg is primitive. With $C(f) = [r]$ and $C(g) = [s]$, we have

$$[1] = C(fg) = C(f)C(g) = [r][s] = [rs].$$

It follows that rs is a unit in R, and so r and s are units in R. Hence f and g are primitive.

(b) This is the special case of part (a) where $g = r$.

(c) Assume that f is irreducible and not constant. Suppose $C(f) = [r]$ where r is not a unit in R. Then there exists a nonconstant primitive polynomial $f_1 \in R[x]$ such that $f = rf_1$. This gives a factorization of f as a product of two nonunits, contradicting the assumption that f is irreducible. □

13. Day 13

This next stuff should all go before this primitive-business.

DEFINITION 13.1. Let R be a UFD, and let $r_1, \ldots, r_n \in R$, not all zero. An element $r \in R$ is a *greatest common divisor (GCD)* of $\{r_1, \ldots, r_n\}$ if (a) $r \big| r_i$ for each i, and (b) if $s \in R$ and $s \big| r_i$ for each i, then $s \big| r$; we write $\gcd(r_1, \ldots, r_n) = [r]$. We say that $r_1, \ldots, r_n$ are *relatively prime* if $\gcd(r_1, \ldots, r_n) = [1]$.

An element $t \in R$ is a *least common multiple (LCM)* of $\{r_1, \ldots, r_n\}$ if (a) $r_i \big| t$ for each i, and (b) if $s \in R$ and $r_i \big| s$ for each i, then $t \big| s$; we write $\operatorname{lcm}(r_1, \ldots, r_n) = [t]$.

LEMMA 13.2. *Let R be a UFD, and let $r_0, \ldots, r_d \in R$, not all zero.*

(a) *There are prime elements $p_1, \ldots, p_n \in R$ and elements $u_0, \ldots, u_d \in R^\times \cup \{0\}$ and $k_{i,j} \in \mathbb{N}$ for $i = 0, \ldots, d$ and $j = 1, \ldots, n$ such that (1) $[p_j] \neq [p_{j'}]$ when $j \neq j'$, and (2) $r_i = u_i p_1^{k_{i,1}} \cdots p_n^{k_{i,n}}$ for each i. If $r_i = 0$, we may take $u_i = 0$ and $k_{i,j} = 0$ for each j.*
(b) *With notation as in part* (a)*, assume $r_0, r_1 \neq 0$. Then $r_0 \big| r_1$ if and only if $k_{0,j} \leqslant k_{1,j}$ for each j.*
(c) *With notation as in part* (a)*, assume $r_0 \neq 0$. Then r_0 is a unit if and only if $k_{0,j} = 0$ for each j.*
(d) *With notation as in part* (a)*, set $m_j = \min\{k_{i,j} \mid r_i \neq 0\}$. Then the element $r = p_1^{m_1} \cdots p_n^{m_n} \in R$ is a GCD for $\{r_0, \ldots, r_d\}$.*
(e) *With notation as in part* (a)*, set $M_j = \max_i\{k_{i,j}\}$. Then the element $t = p_1^{M_1} \cdots p_n^{M_n} \in R$ is an LCM for $\{r_0, \ldots, r_d\}$.*

PROOF. (a) Bookkeeping nightmare: Use the existence of prime factorizations and the uniqueness of prime factorizations.

(b) " $\implies$ " Assume $r_0 \big| r_1$. We will show that $k_{0,1} \leqslant k_{1,1}$, by induction on $k_{0,1}$. (The other cases follow by commutativity of multiplication.)

The base case $k_{0,1} = 0$ is straightforward because $k_{1,1} \geqslant 0$.

So, assume that $k_{0,1} \geqslant 1$.

We will first show that $k_{1,1} \geqslant 1$. Our assumption implies $p_1 \big| r_0$, and since $r_0 \big| r_1$, this implies $p_1 \big| r_1$. Since p_1 is prime, this implies $p_1 \big| u_1$ or $p_1 \big| p_j^{k_{1,j}}$ for some j. Since u_1 is a unit, we have $p_1 \nmid u_1$, and so $p_1 \big| p_j^{k_{1,j}}$ for some j. Then $p_j^{k_{1,j}}$ is not a unit, and so $k_{1,j} \geqslant 1$. It follows that $p_1 \big| p_j$. Since p_j is prime, it is irreducible, so its only factors are the units and the unit multiples of p_j. Since p_1 is not a unit, we conclude that $[p_1] = [p_j]$ and so $1 = j$ by assumption. In particular, we have $k_{1,1} \geqslant 1$.

Let $r_0' = u_0 p_1^{k_{0,1}-1} \cdots p_n^{k_{0,n}}$ and $r_1' = u_0 p_1^{k_{1,1}-1} \cdots p_n^{k_{1,n}}$. Because $p r_0' = r_0 \big| r_1 = p r_1'$, the fact that R is an integral domain implies that $r_0' = r_1'$. By induction, we conclude $k_{0,1} - 1 \leqslant k_{1,1} - 1$, and so $k_{0,1} \leqslant k_{1,1}$.

" $\impliedby$ " Assuming that $k_{0,j} \leqslant k_{1,j}$ for each j, we have

$$r_1' = u_0^{-1} u_1 p_1^{k_{1,1}-k_{0,1}} \cdots p_n^{k_{1,n}-k_{0,n}} \in R$$

and

$$r_0 r_1' = u_0 p_1^{k_{0,1}} \cdots p_n^{k_{0,n}} u_0^{-1} u_1 p_1^{k_{1,1}-k_{0,1}} \cdots p_n^{k_{1,n}-k_{0,n}} = u_1 p_1^{k_{1,1}} \cdots p_n^{k_{1,n}} = r_1$$

and so $r_0 \big| r_1$.

(c) Write $1 = 1 \cdot p_1^0 \cdots p_n^0$. Then r_0 is a unit if and only if $r_0 \big| 1$ if and only if $k_{0,j} \leqslant 0$ for each j by part (b) if and only if $k_{0,j} = 0$.

(d) First, we need to show that $r \big| r_i$ for each i. If $r_i = 0$, then $r_i = 0 = r0 \implies t \big| r_i$. So, assume $r_i \neq 0$. By assumption, we have $k_{i,j} \geqslant m_j$ for each j, and so part (b) implies $r \big| r_i$.

Next, we need to assume that $s \in R$ and $s \big| r_i$ for each i, and show $s \big| r$. Since at least one $r_i \neq 0$, we know $s \neq 0$. If s is a unit, then $s \big| r$ easily. So, assume that s is a nonunit. Write $s = u q_1^{l_1} \cdots q_h^{l_h}$ where u is a unit, $q_1, \ldots, q_h \in R$ are prime and $l_1, \ldots, l_h \geqslant 1$ and $[q_j] \neq [q_{j'}]$ when $j \neq j'$.

Note that each $q_j \big| s$ and $s \big| r_i = u_i p_1^{k_{i,1}} \cdots p_n^{k_{i,n}}$ and so $q_j \big| p_{j'}$ for some j'. Because $p_{j'}$ is irreducible and q_j is not a unit, we conclude that q_j is a unit multiple of $p_{j'}$. Thus, after reordering the q_j we may write $s = v p_1^{l_1} \cdots p_n^{l_n}$ where v is a unit. Now, the assumption

$$v p_1^{l_1} \cdots p_n^{l_n} = s \big| r_i = u_i p_1^{k_{i,1}} \cdots p_n^{k_{i,n}}$$

for each i such that $r_i \neq 0$ implies $l_j \leqslant k_{i,j}$ by part b, and so $l_j \leqslant m_j$. Another application of part (b) implies $s \big| r$.

(e) Similar to part (d). □

LEMMA 13.3. *Let R be a UFD, and let $r_0, \ldots, r_d \in R$, not all zero.*

(a) *Let r be a GCD for $\{r_0, \ldots, r_d\}$. Then r' is a GCD for $\{r_0, \ldots, r_d\}$ if and only if $r' = ur$ for some $u \in R^\times$.*
(b) *Let t be a LCM for $\{r_0, \ldots, r_d\}$. Then t' is an LCM for $\{r_0, \ldots, r_d\}$ if and only if $t' = ut$ for some $u \in R^\times$.*
(c) *With notation as in Lemma 13.2*(d)*, the elements $r_0, \ldots, r_d$ are relatively prime if and only if $m_j = 0$ for each j.*

(d) *If* $\gcd(r_0,\dots,r_d)=[r]$*, then* $r_i/r\in R$ *for all* i *and* $\gcd(r_0/r,\dots,r_d/r)=[1]$.

PROOF. (a) " $\Longrightarrow$ " Assume that r' is a GCD for $\{r_0,\dots,r_d\}$. Since r is also a GCD for $\{r_0,\dots,r_d\}$, we have $r\big|r'$ and $r'\big|r$. Hence, $[r]=[r']$ because R is a domain.

" $\Longleftarrow$ " Assume $r'=ur$ where u is a unit. Since $r\big|r_i$ for all i, we have $r'=ur\big|r_i$ for all i. Also, if $s\big|r_i$ for all i, then $s\big|r$ and $r\big|r'$, so $s\big|r'$. Thus r' is a GCD for $\{r_0,\dots,r_d\}$.

(b) Similar to part (a).

(c) Let r be as in Lemma 13.2(d). Then $\gcd(r_0,\dots,r_d)=[r]$. If $r_0,\dots,r_d$ are relatively prime if and only if $\gcd(r_0,\dots,r_d)=[1]$ if and only if $[r]=[1]$ if and only if r is a unit if and only if each $m_j=0$ by Lemma 13.2(c).

(d) For each i, we have $r\big|r_i$, so we write $r_i=rr_i'$ for some $r_i'\in R$. The cancellation property shows that r_i' is the unique element of R with this property (in fact, it is the unique element of $\mathrm{Q}(R)$ with this property) and so we write $r_i/r=r_i'$.

In the notation of Lemma 13.2, write $r_i=u_ip_1^{k_{i,1}}\cdots p_n^{k_{i,n}}$ for each i and $r=up_1^{m_1}\cdots p_n^{m_n}\in R$. Then $r_i/r=u_iu^{-1}p_1^{k_{i,1}-m_1}\cdots p_n^{k_{i,n}-m_n}$ for each i. For each i and j where $r_i\neq 0$, we have $k_{i,j}\geqslant m_j$, and so $k_{i,j}-m_j\geqslant 0$. And for each j, there is an i such that $r_i\neq 0$ and $k_{i,j}=m_j$. It follows that $\min\{k_{i,j}-m_j\mid r_i/r\neq 0\}=0$ for each j, and so $p_1^0\cdots p_n^0=1$ is a GDC for $\{r_0/r,\dots,r_d/r\}$. □

14. Day 14

LEMMA 14.1. *Let* R *be a UFD and set* $K=\mathrm{Q}(R)$.

(a) *Each element of* K *can be written in the form* a/b *so that* a *and* b *are relatively prime.*
(b) *Let* $0\neq a/b\in K$ *with* $a,b\in R$. *In the notation of Lemma 13.2 write* $a=up_1^{k_1}\cdots p_n^{k_n}$ *and* $b=vp_1^{l_1}\cdots p_n^{l_n}$. *Then* $a/b\in R$ *if and only if* $k_j\geqslant l_j$ *for all* j.
(c) *Given elements* $\frac{a_0}{b_0},\frac{a_1}{b_1},\dots,\frac{a_d}{b_d}\in K$, *there exists an element* $0\neq b\in K$ *such that* $b\frac{a_i}{b_i}\in R$ *for each* i *and* $\gcd(b\frac{a_0}{b_0},b\frac{a_1}{b_1},\dots,b\frac{a_d}{b_d})=[1]$.
(d) *Given elements* $a_0,a_1,\dots,a_d\in R$ *such that* $\gcd(a_0,a_1,\dots,a_d)=[1]$, *if* $c\in K$ *such that* $ca_i\in R$ *for each* i, *then* $c\in R$.

PROOF. (a) Let $c/d\in K$ with $c,d\in R$. If $c/d=0$ then $c/d=0/1$ has the desired form. Assume that $c/d\neq 0$ and let $[r]=\gcd(c,d)$. (Essentially, we will "divide the top and bottom" of $\frac{c}{d}$ by $\gcd(c,d)$ in order to put the fraction in the desired form.) Then $a=c/r$ and $b=d/r$ are elements of R, and Lemma 13.3(d) implies $\gcd(a,b)=[1]$. Furthermore, $\frac{a}{b}=\frac{ar}{br}=\frac{c}{d}$.

(b) Write $c=a/b$ and note that our assumptions imply

$$c=\frac{a}{b}=vw^{-1}p_1^{k_1-l_1}\cdots p_n^{k_n-l_n}.$$

" $\Longleftarrow$ " If $k_j\geqslant l_j$ for all j, then $k_j-l_j\geqslant 0$ and so the above display implies $a/b\in R$.

" $\Longrightarrow$ " Assume $c=a/b\in R$, and suppose that $k_j<l_j$ for some j. Reorder the p_j to assume that $k_1-l_1,\dots,k_t-l_t<0$ and $k_{t+1}-l_{t+1},\dots,k_n-l_n\geqslant 0$. The displayed equality implies

$$p_1^{l_1-k_1}\cdots p_t^{l_t-k_t}c=vw^{-1}p_{t+1}^{k_{t+1}-l_{t+1}}\cdots p_n^{k_n-l_n}.$$

Since p_1 divides the left-hand side, it divides the right-hand side. Thus, $p_1 \big| p_j$ for some $j > 1$, contradicting our assumption $[p_1] \neq [p_j]$.

(c) We use the notation of Lemma 13.2: There are prime elements $p_1, \dots, p_n \in R$ and elements $u_0, \dots, u_d, v_0, \dots, v_d \in R^\times \cup \{0\}$ and $k_{i,j}, l_{i,j} \in \mathbb{N}$ for $i = 0, \dots, d$ and $j = 1, \dots, n$ such that (1) $[p_j] \neq [p_{j'}]$ when $j \neq j'$, and (2) $a_i = u_i p_1^{k_{i,1}} \cdots p_n^{k_{i,n}}$ and $b_i = v_i p_1^{l_{i,1}} \cdots p_n^{l_{i,n}}$ for each i. If $a_i = 0$, we may take $u_i = 0$, $v_i = 1$ and $k_{i,j} = 0 = l_{i,j}$ for each j. Furthermore,

$$\frac{a_i}{b_i} = u_i v_i^{-1} p_1^{k_{i,1} - l_{i,1}} \cdots p_n^{k_{i,n} - l_{i,n}} \in K.$$

Write $M_j = \max_i \{l_{i,j} - k_{i,j}\}$ and set

$$b = p_1^{M_1} \cdots p_n^{M_n}.$$

It follows that we have

$$b \frac{a_i}{b_i} = u_i v_i^{-1} p_1^{M_1 + k_{i,1} - l_{i,1}} \cdots p_n^{M_n + k_{i,n} - l_{i,n}}.$$

To finish the proof we have two things to show.

$b\frac{a_i}{b_i} \in R$ for each i. For this, it suffices to show $M_j + k_{i,j} - l_{i,j} \geqslant 0$ for each j. This inequality follows from the fact that $M_j \geqslant l_{i,j} - k_{i,j}$.

$\gcd(b\frac{a_0}{b_0}, b\frac{a_1}{b_1}, \dots, b\frac{a_d}{b_d}) = [1]$. For this, it suffices to show, for each j, there is an i such that $M_j + k_{i,j} - l_{i,j} = 0$; then apply Lemma 13.3(c). Fix j and choose i such that $M_j = l_{i,j} - k_{i,j}$. This i works.

(d) Write $c = r/s$ so that $\gcd(r, s) = [1]$. Assume without loss of generality that $r/s \neq 0$. There are prime elements $p_1, \dots, p_n \in R$ and elements $u_0, \dots, u_d, v, w \in R^\times \cup \{0\}$ and $k_{i,j}, l_j, m_j \in \mathbb{N}$ for $i = 0, \dots, d$ and $j = 1, \dots, n$ such that (1) $[p_j] \neq [p_{j'}]$ when $j \neq j'$, and (2) $a_i = u_i p_1^{k_{i,1}} \cdots p_n^{k_{i,n}}$ for each i and $r = v p_1^{l_1} \cdots p_n^{l_n}$ and $s = w p_1^{m_1} \cdots p_n^{m_n}$. If $a_i = 0$, we may take $u_i = 0$ and $k_{i,j} = 0$ for each j. Note that, for each j, either $l_j = 0$ or $m_j = 0$ or both. We have

$$c = \frac{r}{s} = v w^{-1} p_1^{l_1 - m_1} \cdots p_n^{l_n - m_n}$$

and, for each i

$$c a_i = \frac{r}{s} a_i = v w^{-1} u_i p_1^{k_{i,1} + l_1 - m_1} \cdots p_n^{k_{i,n} + l_n - m_n}$$

The proof will be complete once we show $l_j \geqslant m_j$ for each j. Our assumption $ca_i \in R$ implies $k_{i,j} + l_j - m_j \geqslant 0$ for each i, j by part (b); that is $l_j \geqslant m_j - k_{i,j}$. The assumption $\gcd(a_0, a_1, \dots, a_d) = [1]$ implies that, for each j there is an i such that $k_{i,j} = 0$. This choice of i yields $l_j \geqslant m_j - 0 = m_j$. □

15. Day 15

Exercise 15.1. Let R be a UFD. If $a, b, c \in R$ and $a \big| bc$ and $\gcd(a, b) = [1]$, then $a \big| c$.

Lemma 15.2. *Let R be a UFD and set $K = \mathrm{Q}(R)$. Let $0 \neq f \in K[x]$.*

(a) *There exists an element $0 \neq b \in \mathrm{Q}(R)$ such that $bf \in R[x]$ and $C(bf) = [1]$.*
(b) *If $c \in K$ and $0 \neq F \in R[x]$ is primitive such that $cF \in R[x]$, then $c \in R$.*
(c) *If $h \in R[x]$ is primitive and $fh \in R[x]$, then $f \in R[x]$.*

PROOF. (a) Write $f = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_d}{b_d}x^d$ with each $a_i, b_i \in R$ and $b_i \neq 0$. Lemma 14.1(c) shows that there exists an element $b \in K$ such that $b\frac{a_i}{b_i} \in R$ for each i and $\gcd(b\frac{a_0}{b_0}, b\frac{a_1}{b_1}, \ldots, b\frac{a_d}{b_d}) = [1]$. In particular, we have $bf \in R[x]$ and $C(bf) = [1]$.

(b) Write $F = a_0 + a_1x + \cdots + a_dx^d$. Since $\gcd(a_0, a_1, \ldots, a_d) = [1]$ and $ca_i \in R$ for each i, Lemma 14.1(d) implies that $c \in R$.

(c) Write $g = fh \in R[x]$ and set $[r] = C(g)$. Let $g_1 \in R[x]$ be primitive such that $g = rg_1$. Use part (a) to find an element $0 \neq c \in \mathrm{Q}(R)$ such that $cf \in R[x]$ and $C(cf) = [1]$. Then $(cr)g_1 = cg = (cf)h \in R[x]$ and the fact that g_1 is primitive implies $cr \in R$. Hence

$$[cr] = [cr]C(g_1) = C(crg_1) = C((cf)h) = C(cf)C(h) = [1][1] = [1]$$

and it follows that cr is a unit in R. Write $cr = u$. In K, it follows that $c^{-1} = ru^{-1} \in R$ and so

$$f = \underbrace{c^{-1}}_{\in R}\ \underbrace{(cf)}_{\in R[x]} \in R[x]$$

as desired. □

THEOREM 15.3. *Let R be a UFD with quotient field $K = \mathrm{Q}(R)$. Let $f \in R[x]$ be primitive. Then f is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$.*

PROOF. ($\Longleftarrow$) Assume that f is irreducible in $K[x]$, and suppose that $f = gh$ with $g, h \in R[x] \subseteq K[x]$. Since f is irreducible in $K[x]$, either g or h is a unit in $K[x]$. Using Exercise 12.1(b), we conclude that either g or h is a constant. By symmetry, assume that g is constant, say $g = r \in R$. By Lemma 12.8(b), since $rh = f$ which is primitive, we know that r is a unit in R, and so g is a unit in $R[x]$.

($\Longrightarrow$) Assume that f is not irreducible in $K[x]$. We will show that f is not irreducible in $R[x]$.

If f is a unit in $K[x]$, then it is constant say $f = r$. Since f is primitive in $R[x]$, we have $[1] = C(f) = [r]$. Hence r is a unit in R and so $f = r$ is a unit in $R[x]$. Thus, in this case, f is not irreducible in $R[x]$.

Assume that f is not a unit in $K[x]$. Since f is nonzero and is not irreducible, there exist nonconstant polynomials $g, h \in K[x]$ such that $f = gh$.

Lemma 15.2(a) implies that there is an element $0 \neq b \in K$ such that $bh \in R[x]$ and $C(bh) = [1]$, that is, $h_1 = bh$ is primitive. Write $g_1 = \frac{1}{b}g \in K[x]$ so that we have $f = gh = (\frac{1}{b}g)(bh) = g_1h_1$. Lemma 15.2(c) implies $g_1 \in R[x]$. That is, we have written $f = g_1h_1$ where g_1, h_1 are nonconstant polynomials in $R[x]$. Hence f is not irreducible in $R[x]$. □

THEOREM 15.4. *If R is a UFD, then $R[x]$ is a UFD.*

PROOF. Set $K = \mathrm{Q}(R)$.

We first show that every nonzero nonunit $f \in R[x]$ can be written as a product of irreducible polynomials in $R[x]$. Since f is a nonzero nonunit, set $C(f) = [c]$ and find a primitive polynomial $f_1 \in R[x]$ such that $f = cf_1$.

Since $K[x]$ is a UFD, we can write $f_1 = p_1 \cdots p_m$ where each $p_i \in K[x]$ is irreducible. Arguing as in Lemma 15.2(c), we can use Lemma 15.2(a) find elements $0 \neq b_1, \ldots, b_m \in K$ such that each $q_i = b_ip_i$ is a primitive polynomial in $R[x]$ and $f_1 = q_1 \cdots q_m$. Notice that b_i is a unit in $K[x]$, so each q_i is irreducible in $K[x]$. Hence, Theorem 15.3 implies that each q_i is irreducible in $R[x]$.

Since R is a UFD, either c is a unit or a product of irreducible elements of R. If c is a unit, then $f = cf_1 = (cq_1)q_2 \cdots q_m$ is a factorization of f in $R[x]$ into a product of irreducibles. If c is not a unit, then there are irreducible elements $r_1, \ldots, r_k \in R$ such that $c = r_1 \cdots r_k$. It is straightforward to show that each r_i is irreducible in $R[x]$: the only way factor a constant polynomial over an integral domain is with constant factors. Hence $f = cf_1 = r_1 \cdots r_k q_1 \cdots q_m$ is a factorization of f in $R[x]$ into a product of irreducibles.

Next we show that an irreducible element $f \in R[x]$ is prime. Lemma 12.8(c), implies that f is either primitive or constant. If f is constant, then the fact that it is irreducible in $R[x]$ implies that it is irreducible in R. Since R is a UFD, f is then prime in R. It is straightforward to show that this implies that f is prime in $R[x]$: since f is prime in R, the ring R/fR is an integral domain, and hence so is $(R/fR)[x] \cong R[x]/(fR[x])$.

Assume that f is primitive. Note that f is irreducible in $K[x]$ by Theorem 15.3. Hence, the fact that $K[x]$ is a UFD implies that f is prime in $K[x]$. Let $g, h \in R[x]$ such that $f \big| gh$ in $R[x]$. It follows that $f \big| gh$ in $K[x]$, and so either $f \big| g$ or $f \big| h$ in $K[x]$ because f is prime in $K[x]$. Assume that $f \big| g$ in $K[x]$ and write $g = fg_1$ for some $g_1 \in K[x]$. Arguing as in Theorem 15.3, we see that g_1 is in $R[x]$, and so $f \big| g$ in $R[x]$, as desired. □

COROLLARY 15.5. *If R is a UFD, then $R[x_1, \ldots, x_n]$ is a UFD.*

PROOF. Induction on n. □

16. Day 16

THEOREM 16.1 (Rational Root Theorem). *Let R be a UFD with $K = \mathrm{Q}(R)$. Let $f = a_0 + a_1 x + \cdots + a_d x^d \in R[x]$ and assume that $r = a/b \in K$ is a root of f with $\gcd(a, b) = [1]$. Then $a \big| a_0$ and $b \big| a_d$. In particular, if f is monic, then $r \in R$.*

PROOF. We have

$$\begin{aligned} 0 &= f(a/b) \\ &= a_0 + a_1(a/b) + \cdots + a_d(a/b)^d \\ 0 &= a_0 b^d + a_1 a b^{d-1} + \cdots + a_{d-1} a^{d-1} b + a_d a^d \\ a_d a^d &= -(a_0 b^d + a_1 a b^{d-1} + \cdots + a_{d-1} a^{d-1} b) \\ &= -b(a_0 b^{d-1} + a_1 a b^{d-2} + \cdots + a_{d-1} a^{d-1}) \end{aligned}$$

and so $b \big| a_d a^d$. Because $\gcd(a, b) = [1]$, Exercise 15.1 implies $b \big| a_d$.

Similarly, we have

$$\begin{aligned} a_0 b^d &= -(a_1 a b^{d-1} + \cdots + a_{d-1} a^{d-1} b + a_d a^d) \\ &= -a(a_1 b^{d-1} + \cdots + a_{d-1} a^{d-2} b + a_d a^{d-1}) \end{aligned}$$

and so $a \big| a_0 b^d$ and $a \big| a_0$.

If f is monic, then $a_d = 1$ and so $b \big| 1$. This implies that b is a unit, so $r = ab^{-1} \in R$. □

EXAMPLE 16.2. The only possible roots of $3x^7 - 7x + 2$ in $\mathbb{Q}$ are $\pm 1, \pm 2, \pm 1/3$ or $\pm 2/3$.

LEMMA 16.3. *Let R be an integral domain, and let $P \subset R$ be a prime ideal. Let $f \in R[x]$ be monic, and let $\overline{f}$ be the polynomial in $R/P[x]$ obtained by reducing the coefficients of f modulo P. If $\overline{f}$ is irreducible in $R/P[x]$, then f is irreducible in $R[x]$.*

PROOF. Observe first that $R/P[x]$ is an integral domain. Since f is monic, so is $\overline{f}$, and $\deg(\overline{f}) = \deg(f)$. Since $\overline{f}$ is irreducible and monic, we have $\deg(\overline{f}) > 0$. Suppose that $f = gh$ for some $g, h \in R[x]$. Since R is an integral domain, we know that the leading coefficient of f is the product of the leading coefficients of g and h. Since f is monic, it follows that the the leading coefficients of g and h are units.

It follows that the leading coefficients of $\overline{g}$ and $\overline{h}$ are units, and $\deg(\overline{g}) = \deg(g)$ and $\deg(\overline{h}) = \deg(h)$. Since $\overline{f}$ is irreducible, we conclude that either $\overline{g}$ or $\overline{h}$ is a unit in $R/P[x]$. Assume by symmetry that $\overline{g}$ is a unit. Since R/P is an integral domain, this implies that $\overline{g}$ is a constant, and so $\deg(g) = \deg(\overline{g}) = 0$. That is, g is a constant, necessarily equal to its leading coefficient, which is a unit. It follows that g is a unit in $R[x]$, so that f is irreducible. □

DEFINITION 16.4. Let I be an ideal in a ring R. Set $I^0 = R$, $I^1 = I$, and inductively $I^{n+1} = II^n$ for $n \geqslant 1$.

PROPOSITION 16.5. *Let R be a UFD with quotient field $K = \mathrm{Q}(R)$, and let $P \subset R$ be a prime ideal. Let $f = a_n x^n + \cdots + a_0 \in R[x]$ with $n \geqslant 1$, and assume that $a_0, \ldots, a_{n-1} \in P$ and $a_0 \notin P^2$ and $a_n \notin P$. Then f is irreducible in $K[x]$. If f is primitive, then f is irreducible in $R[x]$.*

PROOF. Case 1: f is primitive. By Gauss' Lemma, it suffices to show that f is irreducible in $R[x]$. Write $f = gh$ for some $g, h \in R[x]$. We need to show that either g or h is a unit in $R[x]$. Set $k = \deg(g)$ and $l = \deg(h)$.

Case 1a: $k = 0$. Then $g = b_0$ is constant. Since $f = gh = b_0 h$ is primitive, Lemma 12.8(b) implies that b_0 is a unit in R, and so g is a unit in $R[x]$.

Case 1b: $l = 0$. Similar to Case 1a.

Case 1c: $k, l \geqslant 1$. Write $g = b_k x^k + \cdots + b_0$ and $h = c_l x^l + \cdots + c_0$. Since R is an integral domain, we have $n = k + l$. Our assumptions on the a_i imply

$$\overline{b_k}\overline{c_l}x^n + \cdots + \overline{b_0}\overline{c_0} = \overline{g}\overline{h} = \overline{a_n}x^n \neq 0.$$

in $R/P[x]$. It follows that $0 \neq \overline{a_n} = \overline{b_k}\overline{c_l} = \overline{b_k c_l}$ in R/P. Hence $b_k c_l \notin P$ and so $b_k, c_l \notin P$. Let r, s be the smallest integers such that $r \leqslant k$ and $s \leqslant l$ and $b_r \notin P$ and $c_s \notin P$.

Suppose that $r + s = n$. Since $r \leqslant k$ and $s \leqslant l$, this implies $r = k$ and $s = l$, and so $b_0, \ldots, b_{k-1}, c_0, \ldots, c_{l-1} \in P$. It follows that $\overline{g} = \overline{b_k}x^k$ and $\overline{h} = \overline{c_l}x^l$. It follows that $b_0, c_0 \in P$ and so $a_0 = b_0 c_0 \in P^2$, a contradiction.

Thus, we have $r + s < n$. It follows that

$$0 = \overline{a_{r+s}} = \textstyle\sum_{i+j=r+s} \overline{b_i}\overline{c_j}.$$

For $i < r$, we have $\overline{b_i} = 0$ by the choice of r and so $\overline{b_i}\overline{c_j} = 0$. Similarly, for $j < s$, we have $\overline{b_i}\overline{c_j} = 0$. It follows that

$$\overline{b_r}\overline{c_s} = -\sum_{i+j=r+s, i\neq r} \overline{b_i}\overline{c_j} = 0$$

in R/P. Since P is a prime ideal, it follows that either $b_r \in P$ or $c_s \in P$, a contradiction.

Case 2: f is not primitive. By assumption, we have $a_n \notin P$ and so $a_n \neq 0$ and $\deg(f) = n \geqslant 1$. Set $C(f) = [c]$. For each i, set $a_i^* = a_i/c \in R$, and set $f^* = a_n^* x^n + \cdots + a_0^* \in R[x]$. It follows that f^* is primitive, $ca_i^* = a_i$ for each i and $cf^* = f$. In particular, since $ca_n^* = a_n \notin P$, we have $c, a_n^* \notin P$. For $i < n$, we have $ca_i^* = a_i \in P$; since P is prime and $c \notin P$, this implies $a_i^* \in P$. Furthermore, if $a_0^* \in P^2$, then $a_0 = ca_0^* \in P^2$, a contradiction. In particular, it follows that f^* satisfies the hypotheses of the result. By Case 1, it follows that f^* is irreducible in $K[x]$. The fact that $f = cf^*$ is a unit multiple of f^* in $K[x]$, implies that f is irreducible in $K[x]$. □

Corollary 16.6 (Eisenstein's Criterion). *Let R be a UFD with quotient field $K = \mathrm{Q}(R)$, and let $p \in R$ be a prime element. Let $f = a_n x^n + \cdots + a_0 \in R[x]$ with $n \geqslant 1$, and assume that $p \big| a_i$ for $i = 0, \ldots, n-1$ and $p^2 \nmid a_0$ and $p \nmid a_n$. Then f is irreducible in $K[x]$. If f is primitive, then f is irreducible in $R[x]$.*

Proof. Use the prime ideal $P = (p)$ in Proposition 16.5. □

Example 16.7. The polynomial $x^{42} - 37$ is irreducible in $\mathbb{Q}[x]$ and in $\mathbb{Z}[x]$, using $p = 37$.

Example 16.8. Let $p \geqslant 2$ be a prime number. Then the *cyclotomic polynomial* $f = x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible in $\mathbb{Q}[x]$ and in $\mathbb{Z}[x]$, as follows. It is straightforward to show that $(x-1)f = x^p - 1$ and so $f = (x^p - 1)/(x-1)$. It follows that

$$\begin{aligned} f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} &= \frac{x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{i}x^{p-i} + \cdots + \binom{p}{p-1}x}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{i}x^{p-i-1} + \cdots + \binom{p}{p-1}. \end{aligned}$$

Now, recall that $p \big| \binom{p}{i}$ whenever $1 < i < p$, and furthermore that $\binom{p}{p-1} = p$. It follows from Eisenstein's criterion that $f(x+1)$ is irreducible over $\mathbb{Q}$ and over $\mathbb{Z}$, and it is straightforward to show that this implies that f is irreducible over $\mathbb{Q}$ and over $\mathbb{Z}$ as well.

CHAPTER 4

Module Theory I

1. Day 1

DEFINITION 1.1. Let R be a ring. A *(left) R-module* is an additive abelian group M equipped with a map $R \times M \to M$ (denoted $(r, m) \mapsto rm$) such that $(r+s)m = rm + sm$, $r(m+n) = rm + rn$, and $(rs)m = r(sm)$ for all $r, s \in R$ and all $m, n \in M$.

If R has identity, then a left R-module M is *unital* if $1m = m$ for all $m \in M$.

If k is a field, then a *k-vector space* is a unital left k-module.

EXAMPLE 1.2. An abelian group is the same as a unital $\mathbb{Z}$-module.

EXAMPLE 1.3. Let R be a ring. The additive abelian group R^n, consisting of all column vectors of size n with entries in R, is an R-module via the following action

$$r \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} rs_1 \\ \vdots \\ rs_n \end{pmatrix}$$

The set of $m \times n$ matrices with entries in R is denoted $M_{m,n}(R)$. It is also an R-module, with similar coordinate-wise action.

Assume that R has identity. For $j = 1, \ldots, n$ let $e_j \in R^n$ be the vector with ith entry $\delta_{i,j}$. (We call e_j the jth *standard basis vector* of R^n.) In this case the R-modules R^n and $M_{m,n}(R)$ are unital.

EXAMPLE 1.4. Let R be a ring, and let $I \subseteq R$ be an ideal. Then I is an R-module via the multiplication from R. In particular, R is an R-module. Also, the quotient R/I is an R-module via the action $r\overline{s} := \overline{rs}$. (Check that this is well-defined. The other properties are straightforward.) If R has identity, then I and R/I are unital R-modules. Note that I does not need to be a two-sided ideal here.

REMARK 1.5. The previous examples motivate module theory, in that it gives a unification of the theory of abelian groups, the theory of vector spaces, the theory of ideals and the theory of quotients by ideals.

EXAMPLE 1.6. Let R be a ring, and let $\{M_\lambda\}_{\lambda \in \Lambda}$ be a set of R-modules. Then the abelian groups $\prod_\lambda M_\lambda$ and $\oplus_\lambda M_\lambda$ are R-modules via the coordinate-wise action $r(m_\lambda) = (rm_\lambda)$. (See Remark 1.8 to see why $\oplus_\lambda M_\lambda$ is closed under this action.) If R has identity and each M_λ is unital, then $\prod_\lambda M_\lambda$ and $\oplus_\lambda M_\lambda$ are unital.

EXAMPLE 1.7. Let $\varphi\colon R \to S$ be a ring homomorphism. Then S is an R-module via the following action: $rs := \varphi(r)s$. If φ is a homomorphism of rings with identity, then this action makes S into a unital R-module. (Note that this subsumes part of Example 1.4.)

More generally, if M is an S-module, then M has a well-defined R-module structure defined by $rm := \varphi(r)m$. If φ is a homomorphism of rings with identity and M is a unital S-module, then this action makes M into a unital R-module.

In particular, if $I \subset R$ is a two-sided ideal and M is an R/I-module, then M is an R-module via the action $rm := \overline{r}m$. In particular $(R/I)^n$ is an R-module; it is unital when R has identity.

Other examples include:

$(R[x_1, \ldots, x_m])^n$ is an R-module. It is unital when R has identity.

If R is an integral domain with quotient field $K = \mathrm{Q}(R)$, then K^n is a unital R-module.

REMARK 1.8. Let R be a ring and M an R-module. The following properties are straightforward to show:

$r0_M = 0_M$ for all $r \in R$;

$0_R m = 0_M$ for all $m \in M$;

$(-r)m = -(rm) = r(-m)$ for all $r \in R$ and all $m \in M$;

$n(rm) = (nr)m = r(nm)$ for all $n \in \mathbb{Z}$, all $r \in R$ and all $m \in M$.

DEFINITION 1.9. Let R be a ring and let M and N be R-modules. An additive group homomorphism $f\colon M \to N$ is an *R-module homomorphism* if $f(rm) = rf(m)$ for all $r \in R$ and all $m \in M$. An R-module homomorphism is a *monomorphism* if it is 1-1; it is an *epimorphism* if it is onto; and it is an *isomorphism* if it is 1-1 and onto.

The set of all R-module homomorphisms $M \to N$ is denoted $\mathrm{Hom}_R(M, N)$. The category of R-modules and R-module homomorphisms is denoted ${}_R\mathcal{M}$.

If R is a field and M and N are R-vector spaces, then $f\colon M \to N$ is a *linear transformation* if it is an R-module homomorphism.

EXAMPLE 1.10. Let G and H be abelian groups with the natural $\mathbb{Z}$-module structure. A function $f\colon G \to H$ is a $\mathbb{Z}$-module homomorphism if and only if it is a group homomorphism.

EXAMPLE 1.11. Let R be a ring, and let M and N be R-modules. The zero map $M \to N$ given by $m \mapsto 0$ is an R-module homomorphism. The identity map $\mathrm{id}_M\colon M \to M$ given by $m \mapsto m$ is an R-module homomorphism. When R is commutative, for each $r \in R$, the multiplication map $\mu_r\colon M \to M$ given by $m \mapsto rm$ is an R-module homomorphism. The map μ_r is called a *homothety*.

2. Day 2

EXAMPLE 2.1. Let R be a commutative ring with identity. Let R^n and R^m have the natural R-module structure. There is a bijection $\Phi\colon \mathrm{Hom}_R(R^n, R^m) \to M_{m,n}(R)$. Given an R-module homomorphism $f\colon R^n \to R^m$, the associated matrix $\Phi(f)$ is the matrix whose jth column is $f(e_j)$. To see that this is a bijection, we define an inverse $\Psi\colon M_{m,n}(R) \to \mathrm{Hom}_R(R^n, R^m)$. Given an $m \times n$ matrix $(a_{i,j})$ with entries in R, the corresponding R-module homomorphism $\Psi(a_{i,j})$ is the function $f\colon R^n \to R^m$ given by matrix multiplication $f(v) = (a_{i,j})v$.

In particular, the set $\mathrm{Hom}_R(R, R)$ is in bijection with R. That is, the R-module homomorphisms $f\colon R \to R$ are exactly the homotheties $\mu_r\colon R \to R$ given by $s \mapsto rs$.

EXAMPLE 2.2. Let R be a ring and $I \subset R$ a two-sided ideal. Let M and N be R/I-modules, and consider them as R-modules via φ. Then $\mathrm{Hom}_R(M,N) = \mathrm{Hom}_{R/I}(M,N)$. In other words $f\colon M \to N$ is an R-module homomorphism if and only if it is an R-module homomorphism.

Assume that R/I is commutative. Then there is an equality $\mathrm{Hom}_R(R/I, R/I) = \mathrm{Hom}_{R/I}(R/I, R/I)$ which is naturally identified with R/I. That is, the R-module homomorphisms $f\colon R/I \to R/I$ are exactly the homotheties $\mu_r\colon R/I \to R/I$ given by $\overline{s} \mapsto r\overline{s} = \overline{rs}$.

EXAMPLE 2.3. Let $\varphi\colon R \to S$ be a ring homomorphism. If we give S the R-module structure induced by φ, then this makes φ into an R-module homomorphism.

Let M and N be S-modules and consider them as R-modules via φ. Then $\mathrm{Hom}_S(M,N) \subseteq \mathrm{Hom}_R(M,N)$, but we may not have equality; that is, every S-module homomorphism $M \to N$ is also an R-module homomorphism, but not necessarily vice versa.

For instance, let $S = R[x]$ and let $\varphi\colon R \to R[x]$ be the natural inclusion. The function $f\colon R[x] \to R[x]$ given by $\sum_i a_i x^i \mapsto a_0$ is an R-module homomorphism but is not an $R[x]$-module homomorphism.

PROPOSITION 2.4. *Let R be a ring, M an R-module and Λ a set. Given a subset $\{m_\lambda\}_{\lambda\in\Lambda}$, the map $f\colon R^{(\Lambda)} \to M$ given by $(r_\lambda) \mapsto \sum_\lambda r_\lambda m_\lambda$ is a well-defined R-module homomorphism.*

PROOF. It is straightforward to show that f is a well-defined additive group homomorphism. It is an R-module homomorphism because

$$f(r(r_\lambda)) = f((rr_\lambda)) = \textstyle\sum_\lambda (rr_\lambda)m_\lambda = \sum_\lambda r(r_\lambda m_\lambda) = r(\sum_\lambda r_\lambda m_\lambda) = rf(r_\lambda)$$

□

DEFINITION 2.5. Let R be a ring and let M be an R-module. A *R-submodule* of M is an additive subgroup $N \subseteq M$ such that, for all $r \in R$ and all $n \in N$, we have $rn \in N$. If k is a field and M is a k-vector space, then a k-submodule of M is called a *k-subspace*.

EXAMPLE 2.6. Let G be an abelian group considered as a unital $\mathbb{Z}$-module. A subset $H \subseteq G$ is a $\mathbb{Z}$-submodule of G if and only if it is a subgroup.

EXAMPLE 2.7. Let R be a ring and let M and N be R-modules. The subsets $\{0\} \subseteq M$ and $M \subseteq M$ are R-submodules. If $f \in \mathrm{Hom}_R(M,N)$, then $\mathrm{Ker}(f) \subseteq M$ and $\mathrm{Im}(f) \subseteq N$ are R-submodules. If $N' \subseteq N$ is an R-submodule, then $f^{-1}(N') \subseteq M$ is an R-submodule. If $M' \subseteq M$ is an R-submodule, then $f(M') \subseteq N$ is an R-submodule.

Assume that R is commutative. If $r \in R$, then $(0 :_M r) = \{m \in M \mid rm = 0\} \subseteq M$ is an R-submodule, and $rM = \{rm \mid m \in M\} \subseteq M$ is an R-submodule. This follows from the previous paragraph because the homothety $\mu_r\colon M \to M$ is an R-module homomorphism.

EXAMPLE 2.8. Let R be a ring considered as an R-module via its internal multiplication. A subset $I \subseteq R$ is an R-submodule if and only if it is a left ideal.

EXAMPLE 2.9. Let R be a ring, and let $\{M_\lambda\}_{\lambda\in\Lambda}$ be a set of R-modules. Then $\oplus_\lambda M_\lambda \subseteq \prod_\lambda M_\lambda$ is an R-submodule.

EXAMPLE 2.10. Let R be a ring and $I \subset R$ a two-sided ideal. Let M be an R/I-module, and consider M as an R-module via the natural surjection $R \to R/I$. Then the R/I-submodules of M are exactly the R-submodules of M. In particular, the R-submodules of R/I are exactly the left ideals of R/I, that is, the set of all quotients J/I where J is a left ideal of R such that $I \subseteq J$.

EXAMPLE 2.11. Let $\varphi\colon R \to S$ be a ring homomorphism, and let M be an S-module. Consider M as an R-module via φ. Then every S-submodule of M is an R-submodule, but not vice versa.

For instance, let $S = R[x]$ and let $\varphi\colon R \to R[x]$ be the natural inclusion. Then $R \cong \mathrm{Im}(\varphi) \subset R[x]$ is an R-submodule but is not an $R[x]$-submodule.

REMARK 2.12. Let R be a ring and M an R-module. If R has identity and M is unital, then every submodule of M is unital.

EXAMPLE 2.13. Let R be a ring and M an R-module. If $\{M_\lambda\}_{\lambda\in\Lambda}$ is a set of R-submodules of M, then $\cap_\lambda M_\lambda$ is an R-submodule of M; it is also an R-submodule of M_μ for each $\mu \in \Lambda$.

DEFINITION 2.14. Let R be a ring, M an R-module and $X \subseteq M$ a subset. The *submodule of M generated by X* or *spanned by X*, denoted (X), is the intersection of all submodules of M containing X. If $X = \{x_1, \ldots, x_n\}$, then we write $(X) = (x_1, \ldots, x_n)$. If $(X) = M$, then we say that X *generates* or *spans* M as an R-module.

If M has a finite generating set, then it is *finitely generated*. If M can be generated by a single element, then it is *cyclic*.

If $\{M_\lambda\}_{\lambda\in\Lambda}$ is a set of submodules of M, then $(\cup_\lambda M_\lambda)$ is denoted $\sum_\lambda M_\lambda$.

3. Day 3

REMARK 3.1. Let R be a ring, M an R-module, and $X \subseteq M$ a subset. Then (X) is the smallest submodule of M containing X. The R-module M has a generating set, namely M itself.

EXAMPLE 3.2. Let G be an abelian group with the natural unital $\mathbb{Z}$-module structure. The $\mathbb{Z}$-submodule of G generated by a subset X is equal to the subgroup generated by X. In particular G is generated by X as an $\mathbb{Z}$-module if and only if it is generated by X as an abelian group.

EXAMPLE 3.3. If R is a ring and M is an R-module, then $(\emptyset) = \{0\}$.

EXAMPLE 3.4. If R is a ring with identity, then $R^n = (e_1, \ldots, e_n)$.

EXAMPLE 3.5. Let R be a ring and $I \subset R$ a two-sided ideal. Let M be an R/I-module with the R-module structure coming from the natural surjection $R \to R/I$. For each subset $X \subseteq M$, the R-submodule of M generated by X equals the R/I-submodule of M generated by X. In particular M is generated by X as an R-module if and only if it is generated by X as an R/I-module.

PROPOSITION 3.6. *Let R be a ring with identity and M a unital R-module.*

(a) *Let $X \subseteq M$. There is an equality*

$$(X) = \{\textstyle\sum_{x\in X}^{finite} r_x x \mid r_x \in R, x \in X\}.$$

The function $f\colon R^{(X)} \to (X)$ given by $\sum_x^{finite} r_x e_x \mapsto \sum_x^{finite} r_x x$ is a well-defined R-module epimorphism.

(b) *For each $m_1, \dots, m_n \in M$, we have*

$$(m_1, \dots, m_n) = \{\textstyle\sum_{i=1}^n r_i m_i \mid r_1, \dots, r_n \in R\}$$

and the function $f\colon R^n \to (m_1, \dots, m_n)$ given by $\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \mapsto \sum_{i=1}^n r_i m_i$ is a well-defined R-module epimorphism.

(c) *Given a set $\{M_\lambda\}_{\lambda\in\Lambda}$ of submodules of M, there is an equality*

$$\textstyle\sum_\lambda M_\lambda = \{\sum_\lambda^{finite} m_\lambda \mid m_\lambda \in M_\lambda\}$$

and the function $f\colon \oplus_\lambda M_\lambda \to \sum_\lambda M_\lambda$ given by $(m_\lambda) \mapsto \sum_\lambda m_\lambda$ is a well-defined R-module epimorphism.

PROOF. (a) Set $N = \{\sum_x^{\text{finite}} r_x x \mid r_x \in R, x \in X\}$. It is straightforward to show that N is an R-submodule of M containing X, and so $(X) \subseteq N$. For the reverse containment, we have $x \in X \subseteq (X)$ for each i; since (X) is an R-module, we have $r_x x \in (X)$ for each $r_x \in R$ and furthermore $\sum_x^{\text{finite}} r_x x \in (X)$. This shows $(X) \supseteq N$ and so $(X) = N$.

The function f is a well-defined R-module homomorphism by Proposition 2.4, and it is surjective by the description of (X).

Part (b) is a special case of (a) using $X = \{m_1, \dots, m_n\}$. Part (c) is proved like (a). □

EXAMPLE 3.7. Let R be a ring with identity and let $f\colon M \to N$ be a homomorphism of unital R-modules. If $M = (X)$, then $f(M) = (f(X))$. More generally, for each subset $X \subseteq M$, we have $f((X)) = (f(X))$.

EXAMPLE 3.8. Let $\varphi\colon R \to S$ be a ring homomorphism. Let M be an S-module with the R-module structure coming from φ. For each subset $X \subseteq M$, the R-submodule of M generated by X is contained in the S-submodule of M generated by X, however they may not be equal.

For instance, let R be a commutative ring with identity. The R-submodule of $R[x]$ generated by 1 is R, and the $R[x]$-submodule of $R[x]$ generated by 1 is $R[x]$.

PROPOSITION 3.9. *Let R be a ring, M an R-module and $N \subseteq M$ an R-submodule. The quotient group M/N has a well-defined R-module structure via the action $r(m+N) := (rm)+N$. If M is unital, then M/N is unital. The natural surjection $\pi\colon M \to M/N$ is an R-module homomorphism with* $\operatorname{Ker}(\pi) = N$.

PROOF. First, show that the action is well-defined: Let $r \in R$ and $m, m' \in M$ such that $m + N = m' + N$. Then $m - m' \in N$ and so $rm - rm' = r(m - m') \in N$ which implies $rm + N = rm' + N$.

The R-module axioms for M/N now follow from the R-module axioms for M. For instance, associativity:

$$r(s(m + N)) = r(sm + N) = r(sm) + N = (rs)m + N = (rs)(m + N).$$

The distributive laws are verified similarly. When R has identity and M is unital, it follows similarly that M/N is unital.

The fact that π is an R-module homomorphism is proved next:

$$\pi(rm) = (rm) + N = r(m + N) = r\pi(n).$$

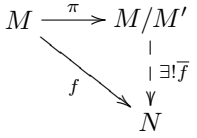
The equality $\operatorname{Ker}(\pi) = N$ was shown in Chapter 1. □

Proposition 3.9 gives one of the best ways to construct R-modules.

EXAMPLE 3.10. Let R be a commutative ring with identity, and let $(a_{i,j}) \in M_{m,n}(R)$. The matrix $(a_{i,j})$ determines an R-module homomorphism $f\colon R^n \to R^m$. It follows that $\operatorname{Im}(f) \subseteq R^m$ is an R-submodule, namely the submodule generated by the columns of $(a_{i,j})$, and so $R^m/\operatorname{Im}(f)$ is an R-module. Proposition 4.1 shows that, in a sense, this is the only way to construct R-modules.

PROPOSITION 3.11. *Let R be a ring, $f\colon M \to N$ an R-module homomorphism, and $M' \subseteq \operatorname{Ker}(f)$ an R-submodule.*

(a) *There is a unique R-module homomorphism $\overline{f}\colon M/M' \to N$ making the following diagram commute*



that is, such that $\overline{f}(m + M') = f(m)$.

(b) *We have $\operatorname{Im}(\overline{f}) = \operatorname{Im}(f)$ and $\operatorname{Ker}(\overline{f}) = \operatorname{Ker}(f)/M'$.*

(c) *$\overline{f}$ is onto if and only if f is onto.*

(d) *$\overline{f}$ is 1-1 if and only if $M' = \operatorname{Ker}(f)$.*

(e) *$\overline{f}$ is an isomorphism if and only if f is onto and $M' = \operatorname{Ker}(f)$. In particular, $\operatorname{Im}(f) \cong M/\operatorname{Ker}(f)$.*

PROOF. (a) Chapter 1 shows that there is a unique group homomorphism making the diagram commute, so we need only show that $\overline{f}$ is an R-module homomorphism:

$$\overline{f}(r(m + M')) = \overline{f}(rm + M') = f(rm) = rf(m) = r\overline{f}(m + M').$$

(b)–(e) These follow from Chapter 1 because they do not depend on the R-module structure. □

4. Day 4

PROPOSITION 4.1. *Let R be a ring with identity and M a unital R-module.*

(a) *There is a set Λ and an R-module epimorphism $\pi\colon R^{(\Lambda)} \to M$. If M is finitely generated, then Λ can be chosen to be finite.*

(b) *There are sets Λ and Γ and an R-module homomorphism $f\colon R^{(\Gamma)} \to R^{(\Lambda)}$ such that $M \cong R^{(\Lambda)}/\operatorname{Im}(f)$. If M is finitely generated, then Λ can be chosen to be finite.*

PROOF. (a) Let Λ be a generating set for R, which exists by Remark 3.1. Note that, if M is finitely generated, then Λ can be chosen to be finite. Proposition 3.6 (a) provides an R-module epimorphism $\pi\colon R^{(\Lambda)} \to (\Lambda) = M$.

(b) Let Λ and π be as in part (a). Then $\operatorname{Ker}(\pi)$ is an R-module, so part (a) implies that there is a set Γ and an R-module epimorphism $\tau\colon R^{(\Gamma)} \to \operatorname{Ker}(\pi)$. Let $\iota\colon \operatorname{Ker}(\pi) \to R^{(\Lambda)}$ be the natural inclusion. Then ι is an R-module homomorphism because $\operatorname{Ker}(\pi) \subseteq R^{(\Lambda)}$ is an R-submodule. It follows that the composition $f = \iota\tau\colon R^{(\Gamma)} \to R^{(\Lambda)}$ is an R-module homomorphism and $\operatorname{Im}(f) = \operatorname{Ker}(\pi)$. This gives the equality in the next sequence

$$M \cong R^{(\Lambda)}/\operatorname{Ker}(\pi) = R^{(\Lambda)}/\operatorname{Im}(f)$$

while the isomorphism is from Proposition 3.11(e). □

The next proposition follows from Chapter 1 material like Proposition 3.11.

PROPOSITION 4.2. *Let R be a ring, M an R-module and $M', M'' \subseteq M$ submodules.*

(a) *There is an R-module isomorphism $M'/(M' \cap M'') \cong (M' + M'')/M''$.*
(b) *If $M'' \subseteq M'$, then $M'/M'' \subseteq M/M''$ is a submodule, and there is an R-module isomorphism $(M/M'')/(M'/M'') \cong M/M'$.*
(c) *Let $\pi\colon M \to M/M''$ be the R-module epimorphism $\pi(m) = m + M''$. There is a 1-1 correspondence*

$$\{\textit{submodules } N \subseteq M \mid M'' \subseteq N\} \longleftrightarrow \{N' \subseteq M/M''\}$$

given by

$$N \longmapsto N/M''$$
$$\pi^{-1}(N') \longmapsfrom N'.$$

(d) *If $M = M' + M''$ and $M' \cap M'' = 0$, then $M \cong M' \oplus M''$.* □

DEFINITION 4.3. Let R be a ring and M an R-module. A subset $X \subseteq M$ is *linear independent* over R if, for every $n \in \mathbb{N}$ and every list of distinct elements $x_1, \ldots, x_n \in X$, given $r_1, \ldots, r_n \in R$ such that $\sum_i r_i x_i = 0$, we have $r_i = 0$ for $i = 1, \ldots, n$.

Assume that R has identity. A subset of $X \subseteq M$ is an *R-basis* for M if it spans M as an R-module and is linearly independent over R. If M has a basis, then it is *free*.

EXAMPLE 4.4. Let G be an abelian group with the natural unital $\mathbb{Z}$-module structure. A subset $X \subseteq G$ is a $\mathbb{Z}$-basis for G if and only if it is a basis for G as an abelian group. In particular G is free as a $\mathbb{Z}$-module if and only if it is free as an abelian group.

EXAMPLE 4.5. If R is a ring with identity and M is a unital R-module, then $\emptyset$ is an R-basis for $\{0\}$.

EXAMPLE 4.6. If R is a ring with identity, then $\{e_1, \ldots, e_n\} \subseteq R^n$ is an R-basis. Hence R^n is a free R-module. More generally, if Λ is a set, then $\{e_\lambda\}_{\lambda \in \Lambda} \subseteq R^{(\Lambda)}$ is an R-basis. Hence $R^{(\Lambda)}$ is a free R-module. We shall see below that, up to isomorphism, these are the only free R-modules.

Most R-modules are not free:

EXAMPLE 4.7. The unital $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ is not free. Indeed, a generating set $X \subseteq \mathbb{Z}/2\mathbb{Z}$ must be nonempty because $\mathbb{Z}/2\mathbb{Z} \neq 0$. However, for each $x \in X$, we have $2x = 0$ in $\mathbb{Z}/2\mathbb{Z}$ even though $2 \neq 0$ in $\mathbb{Z}$; hence X is not linearly independent over $\mathbb{Z}$.

More generally, if R is a ring with identity and $0 \neq I \subsetneq R$ is an ideal, then R/I is not a free R-module. In particular, this shows that quotients of free R-modules need not be free.

Submodules of free R-modules need not be free.

EXAMPLE 4.8. Every subgroup of $\mathbb{Z}^n$ is free as an abelian group by Proposition 1.20.2. In other words, every $\mathbb{Z}$-submodule of $\mathbb{Z}^n$ is free as a $\mathbb{Z}$-module.

Over different rings, though, the analogous result need not be true. Indeed, the $\mathbb{Z}/6\mathbb{Z}$-module $M = \mathbb{Z}/6\mathbb{Z}$ is free as a $\mathbb{Z}/6\mathbb{Z}$-module. However, the $\mathbb{Z}/6\mathbb{Z}$-submodule $3\mathbb{Z}/6\mathbb{Z} \subseteq \mathbb{Z}/6\mathbb{Z}$ is not free as a $\mathbb{Z}/6\mathbb{Z}$-module. (Argue as in Example 4.7.)

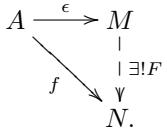
For another example, let k be a field and consider the polynomial ring $R = k[x, y]$. Then R is a free R-module, and the ideal $(x, y) \subset R$ is a submodule. The submodule (x, y) is generated by the set $\{x, y\}$ but this set is not a basis over R because $yx - xy = 0$ and $y \neq 0$. (We will see below that this shows that (x, y) is not free as an R-module.)

EXAMPLE 4.9. Let R be a ring with identity. The polynomial ring $R[x]$, considered as an R-module via the natural inclusion $R \to R[x]$ is a free R-module with basis $\{1, x, x^2, \ldots\}$.

The next result is proved like Proposition 118.7.

PROPOSITION 4.10. *Let R be a ring with identity and M a unital R-module. For a function $\epsilon\colon A \hookrightarrow M$, the following conditions are equivalent:*

(i) *there is an R-module isomorphism $\varphi\colon R^{(A)} \to M$ such that $\varphi(\mathbf{e}_\alpha) = \epsilon(\alpha)$ for each $\alpha \in A$;*
(ii) *$\epsilon(A)$ is a basis for M;*
(iii) *for each unital R-module N and each function $f\colon A \to N$, there is a unique R-module homomorphism $F\colon M \to N$ making the following diagram commute:*



□

LEMMA 4.11. *Let k be a field and V a k-vector space.*

(a) *Let $X \subseteq V$, and let $Y \subseteq X$ be a linearly independent subset that is maximal among all linearly independent subsets of V contained in X, with respect to inclusion. Then Y is a basis for (X).*
(b) *Let $Y \subseteq V$ be a linearly independent subset that is maximal among all linearly independent subsets of V, with respect to inclusion. Then Y spans V and so Y is a basis for V.*

PROOF. (a) The condition $Y \subseteq X$ implies $(Y) \subseteq (X)$. The desired conclusion will follow once we show $(Y) = (X)$, because then Y will be a linearly independent spanning set for (X). So, suppose $(Y) \subset (X)$.

Claim: $X \not\subseteq (Y)$. If not, then $X \subseteq (Y)$ and so $(X) \subseteq ((Y)) = (Y) \subseteq (X)$ which implies $(X) = (Y)$, a contradiction.

Fix an element $v \in X \smallsetminus (Y)$, and set $Y' = Y \cup \{v\}$. We will show that Y' is linearly independent, and this will contradict the maximality of X. Let $r, r_1, \ldots, r_n \in k$ and $y_1, \ldots, y_n \in Y$ such that $rv + \sum_i r_i y_i = 0$. If $r \neq 0$, then $v = \sum_i (-r^{-1} r_i) y_i \in (Y) \subseteq (X)$, a contradiction. It follows that $r = 0$ and so $\sum_i r_i y_i = 0$. Since Y is linearly independent, it follows that $r_i = 0$ for each i. Hence Y' is linearly independent.

(b) This is the special case $X = V$ of part (a). □

5. Day 5

THEOREM 5.1. *Let k be a field and V a k-vector space. Every linearly independent subset of V is contained in a basis for V. In particular V has a basis and is therefore free.*

PROOF. The second statement is the special case $X = \emptyset$ of the first statement, so we prove the first statement.

Let $X \subseteq V$ be a linearly independent subset. Set

$$\Sigma = \{\text{linearly independent } Z \subseteq V \mid X \subseteq Z\}$$

and partially order Σ by inclusion. Since $X \in \Sigma$, we have $\Sigma \neq \emptyset$. We will apply Zorn's Lemma to show that Σ contains a maximal element Y. This will be a linearly independent subset of V that is maximal among all linearly independent subsets of V, with respect to inclusion, that contains X. Then Lemma 4.11(b) will imply that Y is a basis for V containing X.

Let $\mathcal{C}$ be a chain in Σ. That is $\mathcal{C} \subseteq \Sigma$ such that, for all $Z, Z' \in \mathcal{C}$, either $Z \subseteq Z'$ or $Z' \subseteq Z$. It is straightforward to show that the set $\cup_{Z\in\mathcal{C}} Z$ is a linearly independent subset of V such that $X \subseteq \cup_{Z\in\mathcal{C}} Z$, that is, we have $\cup_{Z\in\mathcal{C}} Z \in \Sigma$. It follows immediately that $\cup_{Z\in\mathcal{C}} Z$ is an upper bound for $\mathcal{C}$ in Σ. Thus Σ satisfies the hypotheses of Zorn's Lemma. □

THEOREM 5.2. *Let k be a field and V a k-vector space. Every spanning set for V contains a basis for V.*

PROOF. Let $X \subseteq V$ be a spanning set for V. Set

$$\Sigma = \{\text{linearly independent } Z \subseteq X\}$$

and partially order Σ by inclusion. Since $\emptyset \in \Sigma$, we have $\Sigma \neq \emptyset$. As in the proof of Theorem 5.1, the set Σ contains a maximal element Y. This is a linearly independent subset of V that is maximal among all linearly independent subsets of V contained in X, with respect to inclusion. Lemma 4.11(a) implies that Y is a basis for $(X) = V$ contained in X. □

EXAMPLE 5.3. Let $m, n \geqslant 1$. In Chapter 1 we showed that, if $\mathbb{Z}^m \cong \mathbb{Z}^n$, then $m = n$. If we replace $\mathbb{Z}$ with an arbitrary ring R with identity, though, the analogous statement can be false. (See Hungerford Exercise IV.2.13.) We will see, however, that when R is commutative with identity, this is OK.

First we show that free modules with infinite bases are always OK.

LEMMA 5.4. *Let R be a ring with identity and F a free R-module. If X is a basis for F and $X' \subset X$, then X' does not span F.*

PROOF. Let $x \in X \smallsetminus X'$. We claim that $x \notin (X')$. (Then $x \in F \smallsetminus (X')$ and so X' does not span F.) Suppose $x \in (X')$ and write $x = \sum_{i=1}^{m} r_i x_i'$ with the $r_i \in R$ and $x_i' \in X$. Then the nontrivial linear dependence relation $-x + \sum_{i=1}^{m} r_i x_i' = 0$ contradicts the linear independence of X. □

LEMMA 5.5. *Let R be a ring with identity and F a free R-module. If X spans F and Y is a finite subset of F, then there is a finite subset $X' \subseteq X$ such that $(Y) \subseteq (X')$.*

PROOF. Write $Y = \{y_1, \ldots, y_m\} \subseteq F = (X)$. For each $i = 1, \ldots, m$ there exists $n_i \in \mathbb{N}$ and $x_{i,1}, \ldots, x_{i,n_i} \in X$ and $r_{i,1}, \ldots, r_{i,n_i} \in R$ such that $y_i = \sum_{j=1}^{n_i} r_{i,j} x_{i,j}$. Consider the finite set $X' = \{x_{i,j} \mid i = 1, \ldots, n; j = 1, \ldots, n_i\} \subseteq X$. It follows that $Y \subseteq (X')$ and so $(Y) \subseteq ((X')) = (X')$. □

LEMMA 5.6. *Let R be a ring with identity and F a free R-module. If F has an infinite basis, then every spanning set (and hence every basis) for F is infinite.*

PROOF. Let X be an infinite basis for F, and let Y be a spanning set for F. By way of contradiction, suppose that Y is a finite set. By Lemma 5.5 there is a finite subset $X' \subseteq X$ such that $F = (Y) \subseteq (X') \subseteq F$. Hence $(X') = F$ and so X' spans F. On the other hand, X is infinite and X' is a finite subset. Hence $X' \subset X$, and so Lemma 5.4 says that X' cannot span F, a contradiction. □

LEMMA 5.7. *Let R be a ring with identity and F an R-module. Let X be a linearly independent subset of F and let $X', X'' \subseteq X$. If $(X') \subseteq (X'')$, then $X' \subseteq X''$.*

PROOF. Suppose that $x' \in X' \smallsetminus X''$. Since $x' \in X' \subseteq (X') \subseteq (X'')$ we have $x' = \sum_i r_i x_i''$ for some $r_i \in R$ and distinct $x_i'' \in X''$. Since x' is distinct from the x_i'', this yields a nontrivial linear dependence relation in X, a contradiction. □

REMARK 5.8. Let R be a ring with identity and F a free R-module. Let Y be a basis for F, and let $K(Y)$ denote the set of all finite subsets of Y. Let $X \subseteq F$, and define a function $f\colon X \to K(Y)$ as follows: for each $x \in X$ let $f(x) = \{y_1, \ldots, y_n\}$ where there exist $r_1, \ldots, r_n \in R$ such that each $r_i \neq 0$ and $x = \sum_{i=1}^{n} r_i y_i$. Since Y is a basis for F, the y_i are uniquely determined by x, so this function is well-defined.

LEMMA 5.9. *Let R be a ring with identity and F a free R-module. Assume that X and Y are infinite bases for F, and let $K(Y)$ denote the set of all finite subsets of Y. Let $f\colon X \to K(Y)$ be the function from Remark 5.8.*

(a) *The set $\cup_{S \in \mathrm{Im}(f)} S \subseteq Y$ spans F, and so $\cup_{S \in \mathrm{Im}(f)} S = Y$.*
(b) *The set $\mathrm{Im}(f)$ is infinite.*
(c) *For each $T \in K(Y)$, the set $f^{-1}(T)$ is finite.*

PROOF. (a) For each $x \in X$, we have $x \in (f(x))$ by definition of f. Hence $X \subseteq (\cup_{S \in \mathrm{Im}(f)} S)$ and so $F = (X) \subseteq (\cup_{S \in \mathrm{Im}(f)} S) \subseteq F$ which implies $(\cup_{S \in \mathrm{Im}(f)} S) = F$. Since Y is a basis for F and $\cup_{S \in \mathrm{Im}(f)} S$ is a spanning set for F contained in Y, Lemma 5.4 implies $\cup_{S \in \mathrm{Im}(f)} S = Y$.

(b) Suppose that $\mathrm{Im}(f)$ is finite. Since each element of $\mathrm{Im}(f)$ is a finite subset of Y, it follows that $Y' = \cup_{S \in \mathrm{Im}(f)} S$ is a finite subset of Y. Part (a) says that Y' spans F. On the other hand, Y is infinite and Y' is a finite subset. Hence $Y' \subset Y$, and so Lemma 5.4 says that Y' cannot span F, a contradiction.

(c) Note that $f^{-1}(T) \subseteq X$. If $T \notin \mathrm{Im}(f)$, then $f^{-1}(T) = \emptyset$ which is a finite set. Assume that $T \in \mathrm{Im}(f)$. If $x \in f^{-1}(T)$, then $x \in (T)$ by definition of f. It follows that $f^{-1}(T) \subseteq (T)$. On the other hand, Lemma 5.5 implies that there is a finite subset $X' \subset X$ such that $(T) \subseteq (X')$ and so $(f^{-1}(T)) \subseteq (T) \subseteq (X')$. Since $f^{-1}(T)$ and X' are subsets of X, Lemma 5.7 implies $f^{-1}(T) \subseteq X'$. Since X' is finite, the same is true of $f^{-1}(T)$. □

6. Day 6

Here are some highlights of Hungerford section 0.8.

DEFINITION 6.1. Let X and Y be sets. If there is a 1-1 function $X \to Y$, then we write $|X| \leqslant |Y|$. If there is a bijection $X \to Y$, then we say that X and Y have *the same cardinality* and write $|X| = |Y|$. A set X is countable if $|X| = |\mathbb{N}|$.

EXAMPLE 6.2. When X and Y are finite sets, they have the same cardinality if and only if they contain the same number of elements.

FACT 6.3. (Schroeder-Bernstein Theorem) Let X and Y be sets. If $|X| \leqslant |Y|$ and $|Y| \leqslant |X|$, then $|X| = |Y|$. In other words, if there are 1-1 functions $X \to Y$ and $Y \to X$, then there is a bijection $X \to Y$.

FACT 6.4. Let X be an infinite set. Then $|X \times \mathbb{N}| = |X|$. If $K(X)$ denotes the set of all finite subsets of X, then $|K(X)| = |X|$.

THEOREM 6.5. *Let R be a ring with identity and F a free R-module with an infinite basis X. Then every basis for F has the same cardinality as X. Specifically, if Y is another basis for F, then there is a bijection $X \to Y$.*

PROOF. Let Y be another basis for F. Lemma 5.6 implies that Y is infinite. Let $K(Y)$ denote the set of all finite subsets of Y. Let $f\colon X \to K(Y)$ be the function from Remark 5.8. Note that X is the disjoint union $X = \cup_{T \in \mathrm{Im}(f)} f^{-1}(T)$.

For each $T \in \mathrm{Im}(f)$ order the elements of $f^{-1}(T)$, say $x_1, \ldots, x_n$ are the distinct elements of $f^{-1}(T)$. Define a function $g_T\colon f^{-1}(T) \to \mathbb{N}$ by setting $g_T(x_i) = i$.

Define $h\colon X \to K(Y) \times \mathbb{N}$ by the assignment $h(x) = (f(x), g_{f(x)}(x))$. One checks readily that h is well-defined and 1-1. Using Fact 6.4 this implies

$$|X| \leqslant |K(Y) \times \mathbb{N}| = |K(Y)| = |Y|.$$

By symmetry we have $|Y| \leqslant |X|$, so the Schroeder-Bernstein Theorem implies $|X| = |Y|$, as desired. □

LEMMA 6.6. *Let k be a field and let F be a k-vector space. Fix elements $x_1, \ldots, x_j, y_j, \ldots, y_n \in F$ where $1 \leqslant j < n$, and assume that F is spanned by $\{x_1, \ldots, x_{j-1}, y_j, \ldots, y_n\}$. If $\{x_1, \ldots, x_j\}$ is linearly independent, then the y_i's can be reindexed so that $F = (x_1, \ldots, x_{j-1}, x_j, y_{j+1}, \ldots, y_n)$.*

PROOF. Case 1: $j = 1$. Our assumptions translate as: $F = (y_1, \ldots, y_n)$ and $x_1 \neq 0$. Since $x_1 \in F = (y_1, \ldots, y_n)$ we have $x_1 = r_1 y_1 + \cdots r_n y_n$ for some $r_i \in R$. Since $x_1 \neq 0$, we have $r_k \neq 0$ for some k. Reorder the y_i's to assume that $r_1 \neq 0$. Since k is a field, we have

$$y_1 = r_1^{-1} x_1 + \textstyle\sum_{i=2}^{n} (-r_1^{-1} r_i) y_i$$

and so $y_1 \in (x_1, y_2, \ldots, y_n)$. Since we also have $y_i \in (x_1, y_2, \ldots, y_n)$ for each $i = 2, \ldots, n$, we have

$$F = (y_1, y_2, \ldots, y_n) \subseteq (x_1, y_2, \ldots, y_n) \subseteq F$$

and so $F = (x_1, y_2, \ldots, y_n)$.

Case 2: $j \geqslant 2$. We have $F = (x_1, \ldots, x_{j-1}, y_j, \ldots, y_n)$, and the set $\{x_1, \ldots, x_j\}$ is linearly independent. Since $x_j \in F = (x_1, \ldots, x_{j-1}, y_j, \ldots, y_n)$ we have $x_j = \sum_{i=1}^{j-1} r_i x_i + \sum_{i=j}^{n} r_i y_i$ for some $r_i \in R$.

Suppose that $r_i = 0$ for $i = j, \ldots, n$, then $x_j = \sum_{i=1}^{j-1} r_i x_i \in (x_1, \ldots, x_{j-1})$, which is impossible since $\{x_1, \ldots, x_{j-1}, x_j\}$ is linearly independent. This implies that $r_i \neq 0$ for some $i = j, \ldots, n$. Reorder the y_i's to assume that $r_j \neq 0$. Since k is a field, the argument of Case 1 shows that $y_j \in (x_1, \ldots, x_{j-1}, x_j, y_{j+1}, \ldots, y_n)$ and further that $F = (x_1, \ldots, x_{j-1}, x_j, y_{j+1}, \ldots, y_n)$ as desired. □

THEOREM 6.7. *Let k be a field and let F be a k-vector space. If X and Y are two bases for F, then $|X| = |Y|$.*

PROOF. If either X or Y is infinite, then this follows from Theorem 6.5. Hence we assume that X and Y are both finite. If X is empty, then it is straightforward to show that Y is empty, and conversely. so we assume that $X, Y \neq \emptyset$. Let $x_1, \ldots, x_m$ be the distinct elements of X and let $y_1, \ldots, y_n$ be the distinct elements of Y.

Claim: $n \geqslant m$. (Once this is shown, a symmetric argument will imply $m \geqslant n$ and so $m = n$ and we are done.) Suppose $n < m$. Lemma 6.6 implies that the y_i's can be reordered so that $F = (x_1, y_2, \ldots, y_n)$. By induction on j, Lemma 6.6 implies that the remaining y_i's can be reordered so that $F = (x_1, \ldots, x_j, y_{j+1}, \ldots, y_n)$ for each $j = 1, \ldots, n$. The case $j = n$ says that $F = (x_1, \ldots, x_n)$. In particular, we have $(x_1, \ldots, x_n, x_{n+1}, \ldots, x_m) \subseteq (x_1, \ldots, x_n)$. Lemma 6.6 implies that $\{x_1, \ldots, x_n, x_{n+1}, \ldots, x_m\} \subseteq \{x_1, \ldots, x_n\}$ and so $x_m \in \{x_1, \ldots, x_n\}$. Since $m > n$ and $\{x_1, \ldots, x_m\}$ is linearly independent, this is impossible. □

LEMMA 6.8. *Let R be a ring with identity and $I \subset R$ a two-sided ideal. Let F be a free R-module with basis X, and let $\pi\colon F \to F/IF$ be the canonical epimorphism. Then F/IF is a free R/I-module with basis $\pi(X)$, and $|\pi(X)| = |X|$.*

PROOF. Step 1: $\pi(X)$ generates F/IF. This follows from Example 3.7 since π is an R-module epimorphism.

Step 2: Fix distinct elements $x_1, \ldots, x_n \in X$ and suppose that $r_1, \ldots, r_n \in R$ such that $\sum_{i=1}^n (r_i + I)\pi(x_i) = 0$. We show that each $r_i \in I$. We have

$$IF = \sum_{i=1}^n (r_i + I)(x_i + IF) = \sum_{i=1}^n (r_i x_i + IF) = (\sum_{i=1}^n r_i x_i) + IF$$

and so $\sum_{i=1}^n r_i x_i \in IF$. Write $\sum_{i=1}^n r_i x_i = \sum_j a_j f_j$ for some $a_j \in I$ and $f_j \in F$. Write each $f_j = \sum_k r_{j,k} x_{j,k}$ for some $r_{j,k} \in R$ and $x_{j,k} \in X$. Then

$$\sum_{i=1}^n r_i x_i = \sum_j a_j f_j = \sum_j a_j (\sum_k r_{j,k} x_{j,k}) = \sum_{j,k} (a_j r_{j,k}) x_{j,k}.$$

Thus, we have written the element $\sum_{i=1}^n r_i x_i$ in the form $\sum_l s_l x'_l$ for some $s_l \in I$ and $x'_l \in X$. Re-index if necessary and add terms of the form $0x_i$ and $0x'_l$ if necessary to write

$$\sum_{i=1}^n r_i x_i = \sum_{i=1}^n s_i x_i$$

with the $s_i \in I$. This implies

$$0 = \sum_{i=1}^n (r_i - s_i) x_i$$

so the fact that X is linearly independent implies $r_i = s_i \in I$ for each i.

Step 3: $\pi(X)$ is linearly independent over R/I. (This will show that F/IF is a free R/I-module with basis $\pi(X)$.) Fix distinct elements $x_1, \ldots, x_n \in X$ and suppose that $r_1, \ldots, r_n \in R$ such that $\sum_{i=1}^n (r_i + I)\pi(x_i) = 0$. Step 2 shows that each $r_i \in I$, and so each coefficient $r_i + I = I = 0_{R/I}$.

Step 4: $|\pi(X)| = |X|$. The map $\pi\colon X \to \pi(X)$ is surjective by design. We need to show that it is 1-1. Suppose that $x, x' \in X$ such that $x \neq x'$ and $\pi(x) = \pi(x')$. Then

$$(1 + I)\pi(x) + (-1 + I)\pi(x') = 0$$

and so Step 2 implies that $1, -1 \in I$. This implies $I = R$, contradicting our assumption $I \subset R$. □

7. Day 7

DEFINITION 7.1. Let R be a ring with identity. R satisfies the *invariant basis property* if: for every free R-module F, any two bases of F have the same cardinality. If R has the invariant basis property and F is a free R-module, the *rank* of F is

$$\operatorname{rank}_R(F) = \begin{cases} n & \text{if } F \text{ has a finite basis with exactly } n \text{ elements} \\ \infty & \text{if } F \text{ has an infinite basis.} \end{cases}$$

Every field k has the invariant basis property by Theorem 6.7. The rank of a k-vector space V is often called the *dimension* of V, denoted $\dim_k(V) = \operatorname{rank}_k(V)$. Note that this definition differs from Hungerford's definition.

THEOREM 7.2. *If R is a commutative ring with identity, then R has the invariant basis property.*

PROOF. Let F be a free R-module with bases X and Y. Let $\mathfrak{m} \subset R$ be a maximal ideal. Let $\pi\colon F \to F/\mathfrak{m}F$ be the canonical epimorphism. Lemma 6.8 implies that $F/\mathfrak{m}F$ is a vector space over $R/\mathfrak{m}$ with bases $\pi(X)$ and $\pi(Y)$. Theorem 6.7 then provides the second inequality in the following sequence

$$|X| = |\pi(X)| = |\pi(Y)| = |Y|$$

while the first and third equalities are from Lemma 6.8. □

Now we focus on the basic properties of dimension.

THEOREM 7.3. *Let k be a field. Let V be a k-vector space and let $W \subseteq V$ be a k-subspace.*

(a) $\dim_k(W) \leqslant \dim_k(V)$.
(b) *If* $\dim_k(W) = \dim_k(V)$ *and* $\dim_k(V) < \infty$, *then* $W = V$.
(c) $\dim_k(V) = \dim_k(W) + \dim_k(V/W)$.

PROOF. Let Y be a k-basis for W. Theorem 5.1 provides a basis X for V such that $Y \subseteq X$.

(a) If $\dim_k(V) = \infty$, then we are done, so assume that $\dim_k(V) < \infty$. Then X is finite, and it follows that Y is finite and

$$\dim_k(W) = |Y| \leqslant |X| = \dim_k(V).$$

(b) Since $\dim_k(V) < \infty$, we know that X is finite, and so Y is finite. Since $\dim_k(W) = \dim_k(V)$, we see that Y is a subset of the finite set X with the same number of elements of X, and so $Y = X$. Thus $W = (Y) = (X) = V$.

(c) Claim: The set $Z = \{x + W \in V/W \mid x \in X \smallsetminus Y\}$ is a k-basis for V/W. To see that Z spans V/W, let $v + W \in V/W$. Since $v \in V$, we write $v = \sum_i r_i x_i + \sum_j s_j y_j$ with $r_i, s_j \in R$, $x_i \in X \smallsetminus Y$ and $y_j \in Y$. Then $\sum_j s_j y_j \in W$ and so

$$v + W = (\textstyle\sum_i r_i x_i + \sum_j s_j y_j) + W = (\sum_i r_i x_i) + W \in (\{x_i + W\}) \subseteq (Z).$$

This shows that $V/W \subseteq (Z)$. Since $Z \subseteq V/W$, we have $(Z) \subseteq V/W$ and so $(Z) = V/W$.

Note that, for $x, x' \in X \smallsetminus Y$ we have $x = x'$ if and only if $x + W = x' + W$. The forward implication is straightforward. For the reverse implication, assume $x + W = x' + W$. This implies $x - x' \in W = (Y)$ and so $x - x' = \sum_i r_i y_i$ for some $r_i \in k$ and $y_i \in Y$. Since the set X is linearly independent, this linearly dependence relation implies $x = x'$.

To see that Z is linearly independent over k, let $x_1 + W, \dots, x_n + W$ be distinct elements of V/W and let $r_1, \dots, r_n \in k$ such that $\sum_i r_i(x_i + W) = 0$. Then $\sum_i r_i x_i \in W$, so there are distinct elements $y_1, \dots, y_m \in Y$ and $s_1, \dots, s_m \in k$ such that

$$\textstyle\sum_i r_i x_i = \sum_j s_j y_j.$$

The elements $x_1, \dots, x_n, y_1, \dots, y_m \in X$ are distinct since $Y \cap (X \smallsetminus Y) = \emptyset$, using the previous paragraph. Hence, the displayed linearly dependence relation implies that each $r_i, s_j = 0$. This establishes the claim.

If $\dim_k(V) = \infty$, then X is infinite, and so either Y or $X \smallsetminus Y$ is infinite; in this case, the formula $\dim_k(V) = \dim_k(W) + \dim_k(V/W)$ is satisfied. If $\dim_k(V) < \infty$, then

$$\dim_k(V) = |X| = |Y| + |X \smallsetminus Y| = \dim_k(W) + \dim_k(V/W)$$

as desired. □

Here is the tower rule.

THEOREM 7.4. *Let $K \subseteq L$ be a field extension and let V be an L-vector space. Then $\dim_K(V) = \dim_K(L) \dim_L(V)$. Furthermore $\dim_K(V)$ is finite if and only if $\dim_K(L)$ and $\dim_L(V)$ are both finite.*

PROOF. Note first that K is a subring of L such that $1_K = 1_L$, and so L is a K-vector space via the multiplication in L. Also V is a K-vector space by restriction of scalars.

Let X be a K-basis of L, and let Y be an L basis of V. Note that, for each $x, x' \in X$ and $y, y' \in Y$, if $xy = x'y'$, then $x = x'$ and $y = y'$. This follows from the fact that $x, x' \in X \subseteq L$ and Y is linearly independent over L.

Claim: The set $Z = \{xy \in L \mid x \in X, y \in Y\}$ is a K-basis for V. We first show that Z is linearly independent. Note that any linear dependence relation in Z can be written in the form

$$\textstyle\sum_i \sum_j r_{i,j} x_j y_i = 0$$

for some distinct elements $x_1, \dots, x_n \in X$ and distinct elements $y_1, \dots, y_n \in Y$ and $r_{i,j} \in R$. Since $\sum_j r_{i,j} x_j \in L$ and Y is linearly independent over L, the displayed equation implies that $\sum_j r_{i,j} x_j = 0$ for each i. Since $r_{i,j} \in k$ and X is linearly independent over L, this equation tells us that each $r_{i,j} = 0$.

Next we show that Z spans V as a K-vector space. Let $v \in V$. Since Y is an L-basis for V, we have $v = \sum_i t_i y_i$ for some $t_i \in L$ and $y_i \in Y$. Since X is a K-basis for L, for each i we have $t_i = \sum_j u_{i,j} x_{i,j}$ for some $u_{i,j} \in K$ and $x_{i,j} \in X$. Hence

$$v = \textstyle\sum_i t_i y_i = v = \sum_i (\sum_j u_{i,j} x_{i,j}) y_i = \sum_{i,j} u_{i,j} (x_{i,j} y_i).$$

The desired conclusions follow from the claim since $|Z| = |X \times Y|$. □

COROLLARY 7.5. *Let k be a field and let $f\colon V \to W$ be a linear transformation of k-vector spaces. Then*

$$\dim_k(V) = \dim_k(\mathrm{Im}(f)) + \dim_k(\mathrm{Ker}(f)).$$

PROOF. We have an isomorphism $\mathrm{Im}(f) \cong V/\mathrm{Ker}(f)$ and so Theorem 7.3(c) yields the desired equality. □

CHAPTER 5

Galois Theory

1. Day 1

DEFINITION 1.1. Let R be a ring and let $X \subseteq R$ be a subset. The *subring of R generated by X* is the intersection of all subrings of R containing X.

REMARK 1.2. The subring test can be used to show that the subring generated by a subset $X \subseteq R$ is a subring of R. It is the unique smallest subring of R containing X. If R is commutative, then so is the subring generated by X. If R has identity and $1_R \in X$, then the subring generated by X is a subring with identity 1_R. If R is an integral domain and $1_R \in X$, then the subring generated by X is an integral domain.

DEFINITION 1.3. Let R be a commutative ring with identity and let $A \subseteq R$ be a subring with identity $1_A = 1_R$. Let $X \subseteq R$ be a subset. The *subring of R generated by X over A* is the subring of R generated by $X \cup A$; it is denoted $A[X]$. If $X = \{r_1, \ldots, r_n\}$, then we write $A[r_1, \ldots, r_n]$ for $A[X]$. If $R = A[r_1, \ldots, r_n]$ for some $r_1, \ldots, r_n \in R$, then we say that R is *finitely generated as an A-algebra*.

REMARK 1.4. Let R be a commutative ring with identity and let $A \subseteq R$ be a subring with identity $1_A = 1_R$. Let $X \subseteq R$ be a subset.

The notation $A[r_1, \ldots, r_n]$ does not mean that this is a polynomial ring. When we are dealing with polynomial rings, we will say so explicitly.

If R is finitely generated as an A-module, then it is finitely generated as an A-algebra. The converse does not hold in general: the polynomial ring $A[x]$ is finitely generated as an A-algebra (see Example 1.8) but it is not finitely generated as an A-module.

Since R is commutative with identity and $1 \in A \subseteq A \cup X$, we see that $A[X]$ is a commutative ring with identity such that $1_{A[X]} = 1_R$.

REMARK 1.5. Let R be a commutative ring with identity and let $A \subseteq R$ be a subring with identity $1_A = 1_R$. Let $r_1, \ldots, r_n \in R$.

(a) For each permutation $\sigma \in S_n$, we have $A[r_{\sigma(1)}, \ldots, r_{\sigma(n)}] = A[r_1, \ldots, r_n]$.
(b) We have $A[r_1, \ldots, r_{n-1}][r_n] = A[r_1, \ldots, r_n]$.

THEOREM 1.6. *Let R be a commutative ring with identity and let $A \subseteq R$ be a subring with identity $1_A = 1_R$. Let $X \subseteq R$. For each $n \geqslant 1$ let $A[x_1, \ldots, x_n]$ be the polynomial ring in n variables.*

(a) $A[X] = \{f(r_1, \ldots, r_n) \in R \mid n \geqslant 1,\ f \in A[x_1, \ldots, x_n] \text{ and } r_1, \ldots, r_n \in X\}$.
(b) *Fix an integer $n \geqslant 1$. If $r_1, \ldots, r_n \in R$, then*

$$A[r_1, \ldots, r_n] = \{f(r_1, \ldots, r_n) \in R \mid f \in A[x_1, \ldots, x_n]\}.$$

The map $\varphi\colon A[x_1, \ldots, x_n] \to A[r_1, \ldots, r_n]$ given by $f \mapsto f(r_1, \ldots, r_n)$ is an epimorphism of commutative rings with identity. Hence $A[r_1, \ldots, r_n] \cong$

$A[x_1, \dots, x_n]/I$ *where* I *is the two-sided ideal* $I = \mathrm{Ker}(\varphi)$*. It follows that* R *is finitely generated as an* A*-algebra if and only if it is isomorphic to a quotient of a polynomial ring over* A *in finitely many variables.*

(c) *For each finite subset* $Y \subseteq A[X]$*, there is a finite subset* $X' \subseteq X$ *such that* $A[Y] \subseteq A[X']$*.*

PROOF. (a) Set

$$B = \{f(r_1, \dots, r_n) \in R \mid n \geqslant 1,\ f \in A[x_1, \dots, x_n] \text{ and } r_1, \dots, r_n \in X\}.$$

Each subring $C \subseteq R$ such that $A \cup X \subseteq C$ must contain every product $ar_1^{m_1} \cdots r_n^{m_n}$ with $a \in A$ and $r_i \in X$ and $m_i \geqslant 0$, since it is closed under multiplication; because C is closed under addition, it must contain every finite sum of such elements. Hence $B \subseteq C$ and so $B \subseteq A[X]$. On the other hand, the subring test can be used to show that B is a subring of R that contains $X \cup A$, and so $B \supseteq A[X]$.

(b) The displayed equality is a special case of part (a). The function φ is a well-defined homomorphism of commutative rings with identity by Proposition 3.10.3, and φ is surjective by the displayed equality.

(c) Write $Y = \{y_1, \dots, y_m\}$. By parts (a) and (b), for each y_i there are $x_{i,1}, \dots, x_{i,n_i} \in X$ such that $y_i \in A[x_{i,1}, \dots, x_{i,n_i}]$. Set $X' = \{x_{i,j} \mid i = 1, \dots, m; j = 1, \dots, n_i\} \subseteq X$. It follows that $A \cup Y \subseteq A[X']$ and so $A[Y] \subseteq A[X']$. □

EXAMPLE 1.7. The ring $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \in \mathbb{R} \mid a, b \in \mathbb{Z}\}$ is the subring of $\mathbb{R}$ generated by $\sqrt{10}$ over $\mathbb{Z}$. The ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ is the subring of $\mathbb{C}$ generated by i over $\mathbb{Z}$.

EXAMPLE 1.8. Let R be a commutative ring with identity and let $R[x_1, \dots, x_n]$ be the polynomial ring in n variables. The subring of $R[x_1, \dots, x_n]$ generated by $x_1, \dots, x_n$ over R is exactly $R[x_1, \dots, x_n]$. In a sense, this justifies the similarity in notation between rings generated by elements and polynomial rings.

2. Day 2

DEFINITION 2.1. The *degree* of a field extension $K \subseteq L$ is $[L : K] = \dim_K(L)$. The extension is *finite* if $[L : K] < \infty$. If F is a field such that $K \subseteq F$ and $F \subseteq L$ are subfields, then F is an *intermediate field* of K and L.

The tower rule translates to the following.

COROLLARY 2.2. *If* $k \subseteq K \subseteq L$ *are field extensions, then* $[L : k] = [L : K][K : k]$*, and the extension* $k \subseteq L$ *is finite if and only if the extensions* $k \subseteq K$ *and* $K \subseteq L$ *are both finite.* □

DEFINITION 2.3. Let K be a field and let $Y \subseteq K$ be a subset. The *subfield of* K *generated by* Y is the intersection of all subfields of K containing Y.

REMARK 2.4. If K is a field and $Y \subseteq K$ is a subset, then the subfield generated by Y is a subfield of K, moreover, it is the unique smallest subfield of K that contains Y.

DEFINITION 2.5. Let $k \subseteq K$ be a field extension and let $X \subseteq K$ be a subset. The *subfield of* K *generated by* X *over* k is the subfield of K generated by $X \cup k$; it is denoted $k(X)$. If $X = \{r_1, \dots, r_n\}$, then we write $k(r_1, \dots, r_n)$ for $k(X)$. If $K = k(r_1, \dots, r_n)$ for some $r_1, \dots, r_n \in K$, we say that K is a *finitely generated*

field extension of k. If $K = k(r)$ for some $r \in K$, we say that K is a *simple* field extension of k.

REMARK 2.6. The notation $k(r_1, \ldots, r_n)$ does not mean that this is the field of quotients of a polynomial ring; see Section 3.11. When we are dealing with quotient fields of polynomial rings, we will do so explicitly.

If the field extension $k \subseteq K$ is finite, then it is finitely generated. The converse does not hold in general: the field of fractions $k(x)$ of the polynomial ring $k[x]$ is finitely generated as a field extension of k (see Example 3.2) but the extension $k \subseteq k(x)$ is not finite.

REMARK 2.7. Let $k \subseteq K$ be a field extension and let $r_1, \ldots, r_n \in K$.

(a) For each permutation $\sigma \in S_n$, we have $k(r_{\sigma(1)}, \ldots, r_{\sigma(n)}) = k(r_1, \ldots, r_n)$.
(b) We have $k(r_1, \ldots, r_{n-1})(r_n) = k(r_1, \ldots, r_n)$.

LEMMA 2.8. *Let $\varphi\colon R \to K$ be a homomorphism of commutative rings with identity where K is a field.*

(a) *If R is a field, then φ is a monomorphism.*
(b) *If φ is a monomorphism, then R is an integral domain.*
(c) $\operatorname{Ker}(\varphi) \subset R$ *is a prime ideal.*
(d) *There is a well-defined monomorphism of fields $\psi\colon \mathrm{Q}(R/\operatorname{Ker}(\varphi)) \to K$ given by $\psi(\overline{r}/\overline{s}) = \varphi(r)\varphi(s)^{-1}$.*

PROOF. (a) $\operatorname{Ker}(\varphi) \subseteq R$ is an ideal of R. Since R is a field, either $\operatorname{Ker}(\varphi) = R$ or $\operatorname{Ker}(\varphi) = (0)$. Since $\varphi(1) = 1 \neq 0$, we have $\operatorname{Ker}(\varphi) \neq R$ and so $\operatorname{Ker}(\varphi) = (0)$.

(b) $\operatorname{Im}(\varphi)$ is a subring of K with the same multiplicative identity as K. Hence $\operatorname{Im}(\varphi)$ is an integral domain. Since φ is a monomorphism, we have $R \cong \operatorname{Im}(\varphi) \subseteq K$, and so R is an integral domain.

(c) The map φ induces a well-defined monomorphism of commutative rings with identity $\overline{\varphi}\colon R/\operatorname{Ker}(\varphi) \to K$ given by $\overline{\varphi}(\overline{r}) = \varphi(r)$. Part (b) implies that $R/\operatorname{Ker}(\varphi)$ is an integral domain, and so $\operatorname{Ker}(\varphi) \subset R$ is a prime ideal.

(d) Case 1: φ is a monomorphism. Note that part (b) implies, in this case, that R is an integral domain. We show that the map $\psi\colon \mathrm{Q}(R) \to K$ given by $\psi(r/s) = \varphi(r)\varphi(s)^{-1}$ is a well-defined homomorphism of commutative rings with identity; then part (a) implies that ψ is a monomorphism.

Well-defined: Let $r/s = r'/s' \in \mathrm{Q}(R)$. Then $s, s' \neq 0$ and $rs' = r's$. We have

$$\varphi(r)\varphi(s') = \varphi(rs') = \varphi(r's) = \varphi(r')\varphi(s).$$

Since φ is a monomorphism, we have $\varphi(s), \varphi(s') \neq 0$. Since K is a field, the displayed equations imply

$$\varphi(r)\varphi(s)^{-1} = \varphi(r')\varphi(s')^{-1}$$

and so ψ is well-defined.

ψ is a homomorphism of commutative rings with identity:

$$\psi\left(\frac{r}{s}+\frac{t}{u}\right)=\psi\left(\frac{ru+ts}{su}\right)=\frac{\varphi(ru+ts)}{\varphi(su)}=\frac{\varphi(r)\varphi(u)+\varphi(t)\varphi(s)}{\varphi(s)\varphi(u)}$$
$$=\frac{\varphi(r)}{\varphi(s)}+\frac{\varphi(t)}{\varphi(u)}=\psi\left(\frac{r}{s}\right)+\psi\left(\frac{t}{u}\right)$$
$$\psi\left(\frac{r}{s}\frac{t}{u}\right)=\psi\left(\frac{rt}{su}\right)=\frac{\varphi(rt)}{\varphi(su)}=\frac{\varphi(r)\varphi(t)}{\varphi(s)\varphi(u)}=\frac{\varphi(r)}{\varphi(s)}\frac{\varphi(t)}{\varphi(u)}=\psi\left(\frac{r}{s}\right)\psi\left(\frac{t}{u}\right)$$
$$\psi(1_{\mathrm{Q}(R)})=\psi\left(\frac{1_R}{1_R}\right)=\frac{\varphi(1_R)}{\varphi(1_R)}=\frac{1_K}{1_K}=1_K$$

Case 2: in general. The map φ induces a well-defined monomorphism of commutative rings with identity $\overline{\varphi}\colon R/\operatorname{Ker}(\varphi)\to K$ given by $\overline{\varphi}(\overline{r})=\varphi(r)$. Part (b) implies that $R/\operatorname{Ker}(\varphi)$ is an integral domain. Case 1 implies that there is a well-defined monomorphism of fields $\psi\colon \mathrm{Q}(R/\operatorname{Ker}(\varphi))\to K$ given by $\psi(\overline{r}/\overline{s})=\overline{\varphi}(\overline{r})\overline{\varphi}(\overline{s})^{-1}$. Since $\overline{\varphi}(\overline{r})\overline{\varphi}(\overline{s})^{-1}=\varphi(r)\varphi(s)^{-1}$, we have the desired monomorphism. □

THEOREM 2.9. *Let $k\subseteq K$ be a field extension and let $X\subseteq K$.*

(a)
$$k(X)=\left\{\frac{f(r_1,\dots,r_n)}{g(r_1,\dots,r_n)}\in K\;\middle|\;\begin{array}{l}n\geqslant 1;\ f,g\in k[x_1,\dots,x_n];\\ r_1,\dots,r_n\in X;\ \text{and } g(r_1,\dots,r_n)\neq 0\end{array}\right\}.$$

(b) *Fix an integer $n\geqslant 1$. Let $k[x_1,\dots,x_n]$ be the polynomial ring in n variables. If $r_1,\dots,r_n\in R$, then*
$$k(r_1,\dots,r_n)=\left\{\frac{f(r_1,\dots,r_n)}{g(r_1,\dots,r_n)}\in K\;\middle|\;\begin{array}{l}f,g\in k[x_1,\dots,x_n]\\ \text{and } g(r_1,\dots,r_n)\neq 0\end{array}\right\}.$$
Let $\varphi\colon k[x_1,\dots,x_n]\to k(r_1,\dots,r_n)$ be the evaluation map given by the rule $f\mapsto f(r_1,\dots,r_n)$. Then $\operatorname{Ker}(\varphi)\subset k[x_1,\dots,x_n]$ is a prime ideal, and φ induces an isomorphism $k(r_1,\dots,r_n)\cong \mathrm{Q}(k[x_1,\dots,x_n]/\operatorname{Ker}(\varphi))$. It follows that the extension $k\subseteq K$ is finitely generated if and only if $K\cong \mathrm{Q}(k[x_1,\dots,x_n]/P)$ for some $n\geqslant 0$ and some prime ideal $P\subset k[x_1,\dots,x_n]$.

(c) *For each finite subset $Y\subseteq k(X)$, there is a finite subset $X'\subseteq X$ such that $k(Y)\subseteq k(X')$.*

PROOF. (a) Set
$$B=\left\{\frac{f(r_1,\dots,r_n)}{g(r_1,\dots,r_n)}\in K\;\middle|\;\begin{array}{l}n\geqslant 1;\ f,g\in k[x_1,\dots,x_n];\\ r_1,\dots,r_n\in X;\ \text{and } g(r_1,\dots,r_n)\neq 0\end{array}\right\}.$$
Each subfield $L\subseteq K$ such that $k\cup X\subseteq L$ must contain every product $ar_1^{m_1}\cdots r_n^{m_n}$ with $a\in k$ and $r_i\in X$ and $m_i\geqslant 0$, since it is closed under multiplication; because L is closed under addition, it must contain every finite sum of such elements; because L is closed under multiplicative inverses of nonzero elements, it must contain every quotient of such sums, provided the denominator is nonzero. Hence $B\subseteq L$ and so $B\subseteq k(X)$. On the other hand, the subring test can be used to show that B is a subring of R that contains $X\cup k$, and so $B\supseteq k(X)$.

(b) The displayed equality is a special case of part (a). The map φ is a well-defined homomorphism of commutative rings with identity by Proposition 3.10.3.

Hence, $\mathrm{Ker}(\varphi) \subset k[x_1, \ldots, x_n]$ is a prime ideal by Lemma 2.8(c). Lemma 2.8(d) provides a well-defined monomorphism of fields

$$\psi\colon \mathrm{Q}(k[x_1, \ldots, x_n]/\mathrm{Ker}(\varphi)) \to k(r_1, \ldots, r_n)$$
$$\psi(\overline{f}/\overline{g}) = \varphi(f)\varphi(g)^{-1} = f(r_1, \ldots, r_n)g(r_1, \ldots, r_n)^{-1}.$$

This map is onto by the explicit description of $k(r_1, \ldots, r_n)$, and hence is an isomorphism.

(c) Write $Y = \{y_1, \ldots, y_m\}$. By parts (a) and (b), for each y_i there are $x_{i,1}, \ldots, x_{i,n_i} \in X$ such that $y_i \in k(x_{i,1}, \ldots, x_{i,n_i})$. Set $X' = \{x_{i,j} \mid i = 1, \ldots, m; j = 1, \ldots, n_i\} \subseteq X$. It follows that $k \cup Y \subseteq k(X')$ and so $k(Y) \subseteq k(X')$. □

3. Day 3

Example 3.1. We have $\mathbb{C} = \mathbb{R}(i)$. The containment $\mathbb{C} \supseteq \mathbb{R}(i)$ is by definition: $\mathbb{R}(i)$ is the smallest subfield of $\mathbb{C}$ that contains $\mathbb{R}$ and i. For the containment $\mathbb{C} \subseteq \mathbb{R}(i)$, note that $\mathbb{R}(i)$ is closed under addition and multiplication. Hence, each element of $\mathbb{C}$, which has the form $a + bi$ is in $\mathbb{R}(i)$.

Example 3.2. Let k be a field and let $k[x_1, \ldots, x_n]$ be the polynomial ring in n variables. The subring of $\mathrm{Q}(k[x_1, \ldots, x_n])$ generated by $x_1, \ldots, x_n$ over k is exactly $k(x_1, \ldots, x_n)$. In a sense, this justifies the similarity in notation between subfields generated by elements and fields of fractions of polynomial rings. In the future, we'll call $k(x_1, \ldots, x_n)$ the *field of rational functions* in n variables over k.

Definition 3.3. Let $K \subseteq L$ be a field extension. An element $u \in L$ is *algebraic* over K if there exists a polynomial $0 \neq f \in K[x]$ such that $f(u) = 0$. If $u \in L$ is not algebraic over K, it is *transcendental* over K. The extension $K \subseteq L$ is *algebraic* if every element of L is algebraic over K; it is *transcendental* if it is not algebraic.

Remark 3.4. Let $K \subseteq K' \subseteq L$ be field extensions. Every element of K is algebraic over K, and so $K \subseteq K$ is an algebraic extension. If the element $u \in L$ is algebraic over K, then u is algebraic over K' since $K[x] \subseteq K'[x]$. If L is algebraic over K, then L is algebraic over K'. If $u \in L$ is algebraic over K, then u is a root of a *monic* polynomial $f \in K[x]$.

Example 3.5. The extension $\mathbb{R} \subseteq \mathbb{C}$ is algebraic: each complex number $a+bi \in \mathbb{C}$ is a root of the polynomial $(x-(a+bi))(x-(a-bi)) = x^2-2ax+(a^2+b^2) \in \mathbb{R}[x]$. We will see below that this can be deduced directly from the fact that i is algebraic over $\mathbb{R}$ and $\mathbb{C} = \mathbb{R}(i)$.

The extension $\mathbb{Q} \subseteq \mathbb{R}$ is transcendental because e and π are transcendental over $\mathbb{Q}$. (This is a highly nontrivial fact.) Notice that $\mathbb{R}$ does contain nontrivial elements that are algebraic over $\mathbb{Q}$, for instance $\sqrt{2}$. Thus, if $K \subseteq L$ is a transcendental extension, then L may contain a mix of algebraic and transcendental elements.

Example 3.6. Let k be a field, and let $k(x_1, \ldots, x_n)$ be the field of rational functions in n variables over k. The extension $k \subseteq k(x_1, \ldots, x_n)$ is transcendental. In fact, every element of $k(x_1, \ldots, x_n) \smallsetminus k$ is transcendental over k.

Simple extensions are divided into two cases: those generated by a transcendental element and those generated by an algebraic element.

Theorem 3.7. *Let $K \subseteq L$ be a field extension, and let $u \in L$ be algebraic over K. Let $K[x]$ be the polynomial ring in one variable over K, and let $\alpha\colon K \to K[x]$ be the natural monomorphism.*

(a) *Then* $K(u) = K[u]$.
(b) *The evaluation map* $\varphi\colon K[x] \to K(u)$ *given by* $f \mapsto f(u)$ *is an epimorphism with* $\mathrm{Ker}(\varphi) = (g)$ *for a unique irreducible (non-constant) monic polynomial* $g \in K[x]$.
(c) *There is an isomorphism of fields* $\psi\colon K[x]/(g) \to K(u)$ *which is the identity on* K*, that is, such that the following diagram commutes*

$$\begin{array}{ccc} K[x] & \xleftarrow{\ \alpha\ } & K \\ {\scriptstyle\pi}\downarrow & & \downarrow \\ K[x]/(g) & \xrightarrow[\cong]{\ \psi\ } & K(u) \end{array}$$

where π *is the natural epimorphism and the unlabeled arrow is inclusion.*

PROOF. The map φ is a homomorphism of commutative rings with identity. Since $K(u)$ is a field, Lemma 2.8(c) implies that $\mathrm{Ker}(\varphi) \subseteq K[x]$ is a prime ideal. Since u is algebraic over K, we have $\mathrm{Ker}(\varphi) \neq 0$. The ring $K[x]$ is a PID, and so $\mathrm{Ker}(\varphi) = (g)$ for some $g \in K[x]$. Since $\mathrm{Ker}(\varphi) = (g)$ is prime and nonzero, it follows that g is irreducible. Since K is a field, we may multiply g by the inverse of its leading coefficient to assume that g is monic. The proof of Theorem 3.8.3 shows that $\mathrm{Ker}(\varphi) = (g)$ is maximal, and so $K[x]/(g)$ is a field. It follows that $\mathrm{Im}(\varphi) \cong K[x]/(g)$ is a subfield of $K(u)$ that contains K and u. Since $K(u)$ is the unique smallest such subfield, we have $K[x]/(g) \cong \mathrm{Im}(\varphi) = K(u)$. From Theorem 1.6(b) we know $K[u] = \mathrm{Im}(\varphi) = K(u)$. This establishes parts (a) and (c).

To finish the proof of part (b), we need to show that g is unique. Suppose that $h \in K[x]$ is an irreducible monic polynomial such that $(h) = (g)$. It follows that $g \big| h$ and $h \big| g$. Since $K[x]$ is an integral domain, we conclude that $h = vg$ for some unit $v \in K[x]$, that is, for a nonzero element $v \in K$. It follows that $\deg(h) = \deg(g)$. Comparing leading coefficients of g and h, we have $1 = 1v$ and so $v = 1$, which implies $h = g$. □

DEFINITION 3.8. With the assumptions of Theorem 3.7: The irreducible monic polynomial g is the *minimal polynomial* or *irreducible polynomial* of u. The *degree* of u over K is $[K(u) : K]$.

4. Day 4

THEOREM 4.1. *Let* $K \subseteq L$ *be a field extension, and let* $u \in L$ *be algebraic over* K*. Let* $K[x]$ *be the polynomial ring in one variable over* K*. Let* $g \in K[x]$ *be the minimal polynomial of* u*, and set* $n = \deg(g) \geqslant 1$.

(a) *If* $f \in K[x]$ *and* $f(u) = 0$*, then* $g \big| f$ *in* $K[x]$.
(b) *The set* $\{1, u, u^2, \ldots, u^{n-1}\}$ *is a* K*-basis for* $K(u)$.
(c) *The degree of* u *over* K *is* $[K(u) : K] = \deg(g) = n$.

PROOF. (a) This is a restatement of the condition $\mathrm{Ker}(\varphi) = (g)$ from Theorem 3.7(b).

(b) We first show that the set $\{1, u, u^2, \ldots, u^{n-1}\}$ spans $K(u)$ as a K-vector space. Let $v \in K(u) = K[u]$. Then $v = f(u)$ for some $f \in K[x]$. The division algorithm in $K[x]$ yields $q, r \in K[x]$ such that $f = qg + r$ and either $r = 0$ or

$\deg(r) < \deg(g)$. In other words, we have $r = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ for some $a_i \in K$. Since $g(u) = 0$, we have

$$v = f(u) = q(u)g(u) + r(u) = 0g(u) + r(u) = a_0 + a_1 u + \cdots + a_{n-1}u^{n-1}$$

and so v is in the K-span of $\{1, u, u^2, \ldots, u^{n-1}\}$. Since v is an arbitrary element of $K(u)$, we have $K(u) \subseteq (1, u, u^2, \ldots, u^{n-1}) \subseteq K(u)$, and so $\{1, u, u^2, \ldots, u^{n-1}\}$ spans $K(u)$.

Next we show that the set $\{1, u, u^2, \ldots, u^{n-1}\}$ is linearly independent over K. Suppose that $\sum_{i=0}^{n-1} b_i u^i = 0$ for some $b_i \in K$. Set $f = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. We need to show that $f = 0$. Note that $f(u) = 0$ by construction, and so $g \big| f$ in $K[x]$ by part (a). However, if $f \neq 0$, then $\deg(f) < \deg(g)$, which is impossible. Hence $f = 0$, and the set $\{1, u, u^2, \ldots, u^{n-1}\}$ is a basis.

(c) This follows immediately from part (b). □

EXAMPLE 4.2. The minimal polynomial of $i \in \mathbb{C}$ over $\mathbb{R}$ is $x^2 + 1$ because i is a root of this monic polynomial and is not a root of any polynomial of smaller degree. Hence, we have $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i] \cong \mathbb{R}[x]/(x^2 + 1)$. Similarly, we have

$$\mathbb{Q}(i) = \mathbb{Q}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\} \cong \mathbb{Q}[x]/(x^2 + 1)$$

and

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\} \cong \mathbb{Q}[x]/(x^2 - 2).$$

The previous results show how to use the division algorithm to find inverses and such.

EXAMPLE 4.3. Consider the polynomial $f = x^3 + 2x^2 + 2x + 2 \in \mathbb{Z}[x]$, which has no rational roots by the rational root theorem. Since $\deg(f) = 3$, we conclude that f is irreducible over $\mathbb{Q}$. However, since f has odd degree, one can show that f has a root $u \in \mathbb{R}$. Thus we have

$$\mathbb{Q}(u) = \mathbb{Q}[u] = \{a + bu + cu^2 \in \mathbb{R} \mid a, b, c \in \mathbb{Q}\} \cong \mathbb{Q}[x]/(x^3 + 2x^2 + 2x + 2).$$

Even without having an explicit expression for u, we can do some arithmetic.

(a) Write the element u^4 as a $\mathbb{Q}$-linear combination $a + bu + cu^2$.

Method 1: In $\mathbb{Q}(u)$, we have $u^3 = -2u^2 - 2u - 2$ and so

$$\begin{aligned} u^4 = uu^3 &= -2u^3 - 2u^2 - 2u = -2(-2u^2 - 2u - 2) - 2u^2 - 2u \\ &= 4u^2 + 4u + 4 - 2u^2 - 2u = 2u^2 + 2u + 4 \end{aligned}$$

Method 2: Use the division algorithm to write $x^4 = (x - 2)f + 2x^2 + 2x + 4$ and so

$$u^4 = (u - 2)\underbrace{f(u)}_{=0} + 2u^2 + 2u + 4 = 2u^2 + 2u + 4.$$

(b) Compute $u^{-4} = (u^4)^{-1}$ in $\mathbb{Q}(u)$.

Method 1: Linear algebra. We have $u^4 = 2u^2 + 2u + 4 \neq 0$. We know that $u^{-4} = au^2 + bu + c$:

$$\begin{aligned}
1 = u^4u^{-4} &= (2u^2 + 2u + 4)(au^2 + bu + c)\\
0u^2 + 0u + 1 &= 2au^4 + (2b + 2a)u^3 + (2c + 2b + 4a)u^2 + (2c + 4b)u + 4c\\
0u^2 + 0u + 1 &= 2a(2u^2 + 2u + 4) + (2b + 2a)(-2u^2 - 2u - 2)\\
&\quad + (2c + 2b + 4a)u^2 + (2c + 4b)u + 4c\\
0u^2 + 0u + 1 &= (2c - 2b + 4a)u^2 + (2c)u + (4a - 4b + 4c)\\
c &= 0\\
0u^2 + 0u + 1 &= (-2b + 4a)u^2 + 0u + (4a - 4b)\\
0 &= -2b + 4a\\
b &= 2a\\
1 &= 4a - 4b = 4a - 8a = -4a\\
a &= -\tfrac{1}{4}\\
b &= -\tfrac{1}{2}\\
u^{-4} &= -\tfrac{1}{4}u^2 - \tfrac{1}{2}u.
\end{aligned}$$

Check this:

$$\begin{aligned}
u^4[-\tfrac{1}{4}u^2 - \tfrac{1}{2}u] &= -\tfrac{1}{4}u^3(u^3 + 2u^2) = -\tfrac{1}{4}u^3(-2u - 2)\\
&= \tfrac{1}{2}(u^4 + u^3) = \tfrac{1}{2}(2u^2 + 2u + 4 + u^3)\\
&= \tfrac{1}{2}(2) = 1\checkmark
\end{aligned}$$

Method 2: Euclidean algorithm, i.e., repeated application of the division algorithm. Find polynomials $g, h \in \mathbb{Q}[x]$ such that $1 = (2x^2 + 2x + 4)g + (x^3 + 2x^2 + 2x + 2)h$.

$$\begin{aligned}
x^3 + 2x^2 + 2x + 2 &= (\tfrac{1}{2}x + \tfrac{1}{2})(2x^2 + 2x + 4) - x\\
2x^2 + 2x + 4 &= (-2x - 2)(-x) + 4
\end{aligned}$$

back-substitute

$$\begin{aligned}
4 &= (2x^2 + 2x + 4) + (2x + 2)(-x)\\
&= (2x^2 + 2x + 4)\\
&\quad + (2x + 2)[-(\tfrac{1}{2}x + \tfrac{1}{2})(2x^2 + 2x + 4) + (x^3 + 2x^2 + 2x + 2)]\\
&= (1)(2x^2 + 2x + 4) - (2x + 2)(\tfrac{1}{2}x + \tfrac{1}{2})(2x^2 + 2x + 4)\\
&\quad + (2x + 2)(x^3 + 2x^2 + 2x + 2)\\
&= (-x^2 - 2x)(2x^2 + 2x + 4) + (2x + 2)(x^3 + 2x^2 + 2x + 2)\\
1 &= \tfrac{1}{4}(-x^2 - 2x)(2x^2 + 2x + 4) + \tfrac{1}{4}(2x + 2)(x^3 + 2x^2 + 2x + 2)
\end{aligned}$$

evaluate at $x = u$

$$1 = \tfrac{1}{4}(-u^2 - 2u)(2u^2 + 2u + 4) + \tfrac{1}{4}(2u + 2)\underbrace{(u^3 + 2u^2 + 2u + 2)}_{=f(u)=0}$$

$$1 = (-\tfrac{1}{4}u^2 - \tfrac{1}{2}u)(2u^2 + 2u + 4)$$

Hence, we have $u^{-4} = (2u^2 + 2u + 4)^{-1} = -\tfrac{1}{4}u^2 - \tfrac{1}{2}u$.

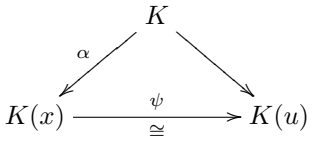
DEFINITION 4.4. Let $K \subseteq L$ and $K \subseteq L'$ be field extensions. A homomorphism of fields $\phi\colon L \to L'$ is a *K-homomorphism* if it is also K-linear, that is, if $\phi(ab) = a\phi(b)$ for all $a \in K$ and all $b \in L$. If ϕ is also bijective, then it is a *K-isomorphism*. Note that, if ϕ is a K-homomorphism, then $\phi(a) = a$ for all $a \in K$ because

$$\phi(a) = \phi(a \cdot 1) = 1\phi(1) = a \cdot 1 = a.$$

In other words, $\phi|_K = \mathrm{id}_K$.

EXAMPLE 4.5. The isomorphism $\psi\colon K[x]/(g) \to K(u)$ from Theorem 3.7(c) is a K-isomorphism, if one identifies K with its image in $K[x]/(g)$.

THEOREM 4.6. *Let $K \subseteq L$ be a field extension. Let $K(x)$ be the field of rational functions is one variable over K, and identify K with its image in $K(x)$ via the natural monomorphism $\alpha\colon K \to K(x)$. If $u \in L$ is transcendental over K, then there is a K-isomorphism of fields $\psi\colon K(x) \to K(u)$ such that $\psi(x) \mapsto u$; in particular, the following diagram commutes*

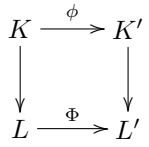


where the unlabeled arrow is inclusion.

PROOF. The evaluation map $\varphi\colon K[x] \to K(u)$ given by $f \mapsto f(u)$ is a monomorphism because u is transcendental over K. Hence, the map $\psi\colon K(x) \to K(u)$ from Theorem 2.9(b), given by $f/g \mapsto f(u)/g(u)$ is a well-defined isomorphism of fields. It follows from the definition of ψ that ψ is the identity on K. □

5. Day 5

Next we discuss the following problem: Given field extensions $K \subseteq L$ and $K' \subseteq L'$, if $\phi\colon K \to K'$ is an isomorphism, when does this "extend" to an isomorphism $\Phi\colon L \to L'$? That is, when does there exist an isomorphism of fields $\Phi\colon L \to L'$ making the following diagram commute:



For example, when $\phi = \mathrm{id}_K\colon K \to K$, Theorems 3.7 and 4.6 showcase certain situations when such a map can be constructed.

THEOREM 5.1. *Let $K \subseteq L$ and $K' \subseteq L'$ be field extensions, and fix $u \in L$ and $u' \in L'$. Let $\phi\colon K \to K'$ be an isomorphism of fields, and assume that u is transcendental over K and that u' is transcendental over K'. Then ϕ extends to an isomorphism $\Phi\colon K(u) \to K'(u')$ such that $\Phi(u) = u'$.*

PROOF. The following diagram is our guide:

$$\begin{array}{ccccccc} K & \longrightarrow & K[x] & \longrightarrow & K(x) & \xleftarrow[\cong]{\psi^{-1}} & K(u) \\ {\scriptstyle\phi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\hat{\phi}}\downarrow{\scriptstyle\cong} & & {\scriptstyle\tilde{\phi}}\downarrow{\scriptstyle\cong} & & \cong\downarrow{\scriptstyle\Phi=\psi'\tilde{\phi}\psi^{-1}} \\ K' & \longrightarrow & K'[x] & \longrightarrow & K'(x) & \xrightarrow[\cong]{\psi'} & K'(u) \end{array}$$

Let $\hat{\phi}\colon K[x] \to K'[x]$ be the induced isomorphism on polynomial rings given by $\sum_i a_i x^i \mapsto \sum_i \phi(a_i)x^i$. Since $\hat{\phi}$ is an isomorphism of integral domains, it induces an isomorphism of quotient fields $\tilde{\phi}\colon K(x) \to K'(x)$ by the formula $\tilde{\phi}(f/g) = \hat{\phi}(f)/\hat{\phi}(g)$. Theorem 4.6 provides isomorphisms $\psi\colon K(x) \to K(u)$ and $\psi'\colon K'(x) \to K'(u')$ such that $\psi(a) = a$ for all $a \in K$ and $\psi'(a') = a'$ for all $a' \in K'$ and $\psi(x) = u$ and $\psi'(x) = u'$. Check that the composition $\Phi = \psi'\tilde{\phi}\psi^{-1}$ has the desired properties. □

THEOREM 5.2. *Let $K \subseteq L$ and $K' \subseteq L'$ be field extensions, and fix $u \in L$ and $u' \in L'$. Let $\phi\colon K \to K'$ be an isomorphism of fields, and let $\hat{\phi}\colon K[x] \to K'[x]$ be the induced isomorphism on polynomial rings. Assume that u is a root of an irreducible polynomial $f \in K[x]$ and that u' is a root of the polynomial $f' = \hat{\phi}(f) \in K[x]$. Then ϕ extends to an isomorphism $\Phi\colon K(u) \to K'(u')$ such that $\Phi(u) = u'$.*

PROOF. The following diagram is our guide:

$$\begin{array}{ccccccc} K & \longrightarrow & K[x] & \longrightarrow & K[x]/(f) & \xleftarrow[\cong]{\psi^{-1}} & K(u) \\ {\scriptstyle\phi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\hat{\phi}}\downarrow{\scriptstyle\cong} & & {\scriptstyle\tilde{\phi}}\downarrow{\scriptstyle\cong} & & \cong\downarrow{\scriptstyle\Phi=\psi'\tilde{\phi}\psi^{-1}} \\ K' & \longrightarrow & K'[x] & \longrightarrow & K'[x]/(f') & \xrightarrow[\cong]{\psi'} & K'(u) \end{array}$$

Since $\hat{\phi}$ is an isomorphism, we know that f' is irreducible over K' and that $\hat{\phi}$ induces an isomorphism of quotients $\tilde{\phi}\colon K[x]/(f) \to K'[x]/(f')$ by the formula $\tilde{\phi}(\overline{g}) = \overline{\hat{\phi}(g)}$. Theorem 3.7 provides isomorphisms $\psi\colon K[x]/(f) \to K(u)$ and $\psi'\colon K'[x]/(f') \to K'(u')$ such that $\psi(a) = a$ for all $a \in K$ and $\psi'(a') = a'$ for all $a' \in K'$ and $\psi(\overline{x}) = u$ and $\psi'(\overline{x}) = u'$. Check that the composition $\Phi = \psi'\tilde{\phi}\psi^{-1}$ has the desired properties. □

COROLLARY 5.3. *Let L and L' be extensions of K, and let $u \in L$ and $u' \in L'$ be algebraic over K. Then u and u' are roots of the same irreducible polynomial $f \in K[x]$ if and only if there is a K-isomorphism $\Phi\colon K(u) \to K(u')$ such that $\Phi(u) = u'$.*

PROOF. $\Longrightarrow$: This is the special case $\phi = \mathrm{id}_K$ of Theorem 5.2.

$\Longleftarrow$: Fix an isomorphism $\Phi\colon K(u) \to K(u')$ such that $\Phi(u) = u'$ and $\Phi(a) = a$ for all $a \in K$. Let $g = \sum_i a_i x^i \in K[x]$ be the minimal polynomial of u over K. Then

$$0 = \Phi(0) = \Phi(f(u)) = \Phi(\textstyle\sum_i a_i u^i) = \sum_i \Phi(a_i)\Phi(u)^i = \sum_i a_i (u')^i = f(u')$$

□

EXAMPLE 5.4. The elements $i, -i \in \mathbb{C}$ are roots of the irreducible polynomial $x^2 + 1 \in \mathbb{R}[x]$. Thus, the conjugation map $\phi\colon \mathbb{C} \to \mathbb{C}$ given by $\phi(a + bi) = a - bi$ is

a well-defined $\mathbb{R}$-isomorphism. Conversely, if $\psi\colon \mathbb{C} \to \mathbb{C}$ is an $\mathbb{R}$-isomorphism, then either $\psi = \mathrm{id}_{\mathbb{C}}$ or $\psi = \phi$.

THEOREM 5.5. *Let K be a field and $f \in K[x]$ a polynomial of degree $n \geqslant 1$. There exists a simple extension $K \subseteq K(u)$ such that*

1. *u is a root of f;*
2. *$[K(u) : K] \leqslant n$ with equality holding if and only if f is irreducible over K; and*
3. *If f is irreducible over K, then $K(u)$ is unique up to K-isomorphism, that is, if $K \subseteq K(u')$ is a simple extension such that u' is a root of f and $[K(u) : K] = n$, then there is a K-isomorphism $\Phi\colon K(u) \to K(u')$ such that $\Phi(u) = u'$.*

PROOF. Assume without loss of generality that $n \geqslant 1$, and write $f = \sum_i a_i x^i$.

Case 1: f is irreducible. Since $K[x]$ is a PID and $f \neq 0$, the ideal $(f) \subset K[x]$ is maximal. Hence, the quotient $K[x]/(f)$ is a field. The composition of natural maps $\phi\colon K \xrightarrow{\epsilon} K[x] \xrightarrow{\pi} K[x]/(f)$ is a homomorphism of fields, so is in particular a monomorphism. Identify K with $\mathrm{Im}(\phi) \subseteq K[x]/(f)$ and let $u = \pi(x)$. Then u is a root of f because

$$f(u) = \textstyle\sum_i a_i u^i = \sum_i a_i \pi(x)^i = \pi(\sum_i a_i x^i) = \pi(f) = 0.$$

Since f is irreducible, it is a constant multiple of the minimal polynomial of u over K. Hence, Theorem 4.1(c) implies that $[K(u) : K] = n$. The uniqueness statement follows from Corollary 5.3.

Case 2: f is reducible. Let g be an irreducible factor of f, and construct the field $K(u) = K[x]/(g)$ as in Case 1. In particular, we have $g(u) = 0$. Since $g \big| f$, this implies $f(u) = 0$. Since f is reducible, we have $n = \deg(f) > \deg(g) = [K(u) : K]$. □

Now we discuss more general algebraic field extensions.

THEOREM 5.6. *Let $K \subseteq L$ be a finite field extension. Then $K \subseteq L$ is finitely generated and algebraic.*

PROOF. Let $[L : K] = n$. If $u_1, \ldots, u_n \in L$ form a K-basis for L, then $L = K(u_1, \ldots, u_n)$, and so the extension is finitely generated. To see that it is algebraic, let $u \in L$. The set $\{1, u, u^2, \ldots, u^n\}$ cannot be linearly independent over K, and so we must have $\sum_{i=0}^{n} a_i u^i = 0$ for some $a_i \in K$. It follows that u is algebraic over K. □

6. Day 6

The next result contains the converse to Theorem 5.6.

THEOREM 6.1. *Let $K \subseteq K(r_1, \ldots, r_n)$ be a finitely generated field extension. The following conditions are equivalent:*

(i) *The elements $r_1, \ldots, r_n$ are algebraic over K;*
(ii) *The extension $K \subseteq K(r_1, \ldots, r_n)$ is finite;*
(iii) *The extension $K \subseteq K(r_1, \ldots, r_n)$ is algebraic.*

PROOF. (i) $\Longrightarrow$ (ii) In the following tower of field extensions, each individual extension is simple and generated by an algebraic element

$$K \subseteq K(r_1) \subseteq K(r_1, r_2) \subseteq \cdots \subseteq K(r_1, \ldots, r_n).$$

Hence, each individual extension in the tower is finite by Theorem 4.1(c). The tower law implies that the extension $K \subseteq K(r_1, \ldots, r_n)$ is also finite.

(ii) $\Longrightarrow$ (iii) Theorem 5.6.

(iii) $\Longrightarrow$ (i) Each $r_1 \in K(r_1, \ldots, r_n)$ is algebraic over K. □

THEOREM 6.2. *Let $K \subseteq L$ be a field extension, and let $X \subseteq L$ be a subset such that $L = K(X)$. The extension $K \subseteq L$ is algebraic if and only if each $r \in X$ is algebraic over K.*

PROOF. ($\Longrightarrow$) Each $r \in X \subseteq L$ is algebraic over K.

($\Longleftarrow$) Assume that each $r \in X$ is algebraic over K. Let $u \in K(X)$. By Theorem 2.9(c) there is a finite list $r_1, \ldots, r_n \in X$ such that $u \in K(r_1, \ldots, r_n)$. Since each r_i is algebraic over K, Theorem 6.1 implies that the extension $K \subseteq K(r_1, \ldots, r_n)$ is algebraic, and so $u \in K(r_1, \ldots, r_n)$ is algebraic over K. Thus, the extension $K \subseteq L$ is algebraic. □

THEOREM 6.3. *Let $K \subseteq L$ and $L \subseteq F$ be field extensions. Then the extension $K \subseteq F$ is algebraic if and only if the extensions $K \subseteq L$ and $L \subseteq F$ are algebraic.*

PROOF. ($\Longrightarrow$) Straightforward using the containment $K[x] \subseteq L[x]$.

($\Longleftarrow$) Let $u \in F$. Since u is algebraic over L, it is a root of some polynomial $\sum_{i=0}^{n} a_i x^i \in L[x]$. Thus, we have $a_i \in L$ and $\sum_{i=0}^{n} a_i u^i = 0$. It follows that u is algebraic over the field $K(a_0, \ldots, a_n)$. Theorem 6.1 implies that the extension $K(a_0, \ldots, a_n) \subseteq K(a_0, \ldots, a_n)(u) = K(a_0, \ldots, a_n, u)$ is finite. Since each a_i is algebraic over K, the extension $K \subseteq K(a_0, \ldots, a_n)$ is finite, so the tower rule implies that the extension $K \subseteq K(a_0, \ldots, a_n, u)$ is finite. Theorem 5.6 implies that the extension $K \subseteq K(a_0, \ldots, a_n, u)$ is algebraic. Since $u \in K(a_0, \ldots, a_n, u)$, we conclude that u is algebraic over K. Since u is an arbitrary element of F, we conclude that the extension $K \subseteq F$ is algebraic. □

THEOREM 6.4. *Let $K \subseteq L$ be a field extension, and set*

$$\overline{K} = \{r \in L \mid r \text{ is algebraic over } K\}.$$

(a) *$\overline{K}$ is an intermediate field of K and L*

(b) *The extension $K \subseteq \overline{K}$ is algebraic. Moreover, $\overline{K}$ is the unique maximal subfield of L that is algebraic over K.*

(c) *Every element of $L - \overline{K}$ is transcendental over $\overline{K}$, and hence over K.*

PROOF. (a) Let $u, v \in \overline{K}$. The extension $K \subseteq K(u, v)$ is algebraic by Theorem 6.1. Hence, the element $u - v \in K(u, v)$ is algebraic over K; that is, $u - v \in \overline{K}$. If $v \neq 0$, then $uv^{-1} \in K(u, v)$ is algebraic over K; that is, $uv^{-1} \in \overline{K}$. It follows readily that $\overline{K}$ is a subfield of L. Since $K \subseteq \overline{K}$, we have the desired conclusion.

(b) By definition, every element of $\overline{K}$ is algebraic over K, and so the extension $K \subseteq \overline{K}$ is algebraic. Since $\overline{K}$ consists of all the elements of L that are algebraic over K, it is the unique maximal subfield of L that is algebraic over K.

(c) If $u \in L - \overline{K}$, then u is not algebraic over K. Hence, it is transcendental over K. If u were algebraic over $\overline{K}$, then $\overline{K}(u)$ would be algebraic over $\overline{K}$. Since $\overline{K}$ is algebraic over K, this would imply that $K \subseteq \overline{K}(u)$ is algebraic by Theorem 6.3, and so u is algebraic over K, a contradiction. □

LEMMA 6.5. *Let k be a field and let V be a finite dimensional k-vector space. Let $f\colon V \to V$ be a linear transformation. The following conditions are equivalent:*

(i) *f is 1-1;*
(ii) *f is onto;*
(iii) *f is an isomorphism.*

PROOF. The implications (iii) $\implies$ (i) and (iii) $\implies$ (ii) are trivial.
(i) $\implies$ (iii) Since f is a monomorphism, we have $V \cong \operatorname{Im}(f)$, and so

$$\dim_k(V/\operatorname{Im}(f)) = \dim_k(V) - \dim_k(\operatorname{Im}(f)) = \dim_k(V) - \dim_k(V) = 0.$$

It follows that $V/\operatorname{Im}(f) = 0$. Hence $V = \operatorname{Im}(f)$ and so f is onto.
(ii) $\implies$ (iii) Since V is onto, we have

$$V = \operatorname{Im}(f) \cong V/\operatorname{Ker}(f).$$

A similar analysis as above shows that $\operatorname{Ker}(f) = 0$ and so f is 1-1. □

REMARK 6.6. This result fails if V is infinite-dimensional. The linear transformation $f\colon k^{(\mathbb{N})} \to k^{(\mathbb{N})}$ given by $f(r_0, r_1, \ldots) = (0, r_0, r_1, \ldots)$ is 1-1 and not onto. The linear transformation $g\colon k^{(\mathbb{N})} \to k^{(\mathbb{N})}$ given by $g(r_0, r_1, \ldots) = (r_1, r_2, \ldots)$ is onto and not 1-1.

THEOREM 6.7. *Let $\varphi\colon k \to R$ be a homomorphism of commutative rings with identity such that k is a field and R is an integral domain. If $\dim_k(R) < \infty$, then R is a field.*

PROOF. Let $0 \neq r \in R$ and consider the map $f\colon R \to R$ given by $f(s) = rs$. Since $r \neq 0$ and R is an integral domain, this map is 1-1. It is straightforward to show that f is a k-linear transformation. Hence, Lemma 6.5 implies that f is an isomorphism. In particular, there is an element $u \in R$ such that $1 = f(u) = ru$. Hence u is a unit in R. Since u is an arbitrary nonzero element of R, this shows that R is a field. □

REMARK 6.8. This conclusion fails to hold if R is infinite-dimensional. The natural inclusion $\varphi\colon k \to k[x]$ into the polynomial ring is a homomorphism of commutative rings with identity such that k is a field and $k[x]$ is an integral domain. However $k[x]$ is not a field.

This conclusion fails to hold if R is not an integral domain. The natural inclusion $\varphi\colon k \to k[x]/(x^2)$ is a homomorphism of commutative rings with identity such that k is a field and $\dim_k(k[x]/(x^2)) = 2 < \infty$. However, $k[x]/(x^2)$ is not an integral domain and hence is not a field.

Note that we also need the integral domain hypothesis in the next result, as $\mathbb{Z}/6$ is a finite commutative ring with identity that is not a field.

THEOREM 6.9. *Every finite integral domain is a field.*

PROOF. (Essentially the same proof as Theorem 6.7.) Let R be a finite integral domain. Let $0 \neq r \in R$ and consider the map $f\colon R \to R$ given by $f(s) = rs$. Since $r \neq 0$ and R is an integral domain, this map is 1-1. Since R is finite and f is 1-1, the pigeon-hole principle implies that f is onto. Hence r is a unit in R. □

THEOREM 6.10. *Let k be a field and fix polynomials $f_1, \ldots, f_n \in k[x]$ of positive degree. There is a finite field extension $k \subseteq K$ such that f_i has a root in K for $i = 1, \ldots, n$. Moreover, there is a field extension $k \subseteq L$ such that each f_i splits into linear factors in $L[x]$.*

PROOF. Set $f = f_1 \cdots f_n$. It suffices to show that there is a field extension $k \subseteq L$ such that each f splits into linear factors in $L[x]$. (This uses the fact that $L[x]$ is a unique factorization domain.) We proceed by induction on $d = \deg(f) \geqslant 1$. The base case $d = 1$ is trivial with $L = k$. Inductively, assume that $d > 1$ and that the result holds for polynomials of degree $< d$. By Theorem 5.5 there is a finite field extension $k \subseteq k(u)$ such that u is a root of f. This implies that $x - u \mid f$ in $k(u)[x]$. Since $k(u)[x]$ is a UFD, we can write $f = (x-u)^m g$ for some $m \geqslant 1$ and some $g \in k(u)[x]$ such that $x - u \nmid g$. If $\deg(g) = 0$, then we are done with $K = k(u)$. So, assume that $\deg(g) \geqslant 1$. Since $\deg(g) = d - m < d$, our induction hypothesis implies that there is a finite field extension $k(u) \subseteq L$ such that g splits into linear factors in $L[x]$. It follows that the extension $k \subseteq L$ is finite and that $f = (x-u)^m g$ splits into linear factors in $L[x]$. □

7. Day 7

We begin by showing that direct limits exist in the category of fields.

PROPOSITION 7.1. *Let $K_1, K_2, \ldots$ be fields, and for $i \geqslant 1$ let $f_i \colon K_i \to K_{i+1}$ be a homomorphism of fields. There exists a field K with homomorphisms of fields $g_i \colon K_i \to K$ satisfying the following properties:*

(1) *For each $i \geqslant 1$, the following diagram commutes*

$$\begin{array}{ccc} K_i & \xrightarrow{f_i} & K_{i+1} \\ & \searrow^{g_i} & \downarrow{\scriptstyle g_{i+1}} \\ & & K. \end{array}$$

(2) *Let L be a field with homomorphisms of fields $h_i \colon K_i \to L$ such that, for each $i \geqslant 1$, the following diagram commutes*

$$\begin{array}{ccc} K_i & \xrightarrow{f_i} & K_{i+1} \\ & \searrow^{h_i} & \downarrow{\scriptstyle h_{i+1}} \\ & & L. \end{array}$$

Then there exists a unique homomorphism of fields $H \colon K \to L$ making each of the following diagrams commute:

$$\begin{array}{ccc} K_i & \xrightarrow{g_i} & K \\ & \searrow^{h_i} & \downarrow{\scriptstyle H} \\ & & L. \end{array}$$

PROOF. Note that, if there is a field F such that $K_1 \subseteq K_2 \subseteq \cdots \subseteq F$ and each map f_i is the inclusion, then $K = \cup_i K_i$ works. Moreover, if there is a field F with homomorphisms of fields $\phi_i \colon K_i \to F$ such that, for each $i \geqslant 1$, the following diagram commutes

$$\begin{array}{ccc} K_i & \xrightarrow{f_i} & K_{i+1} \\ & \searrow^{\phi_i} & \downarrow{\scriptstyle \phi_{i+1}} \\ & & F \end{array}$$

then $K = \cup_i \operatorname{Im}(\phi_i)$ works. (See Proposition 8.2.) The problem in general, though, is that we do not yet know that such a field F exists.

For integers $j \geqslant i \geqslant 1$, define $f_{i,j} \colon K_i \to K_j$ as

$$f_{i,j} = \begin{cases} \mathrm{id}_{K_i} \colon K_i \to K_i & \text{if } j = i \\ f_i \colon K_i \to K_{i+1} & \text{if } j = i+1 \\ f_{j-1} \circ \cdots \circ f_{i+1} \circ f_i \colon K_i \to K_j & \text{if } j > i+1. \end{cases}$$

Let

$$A = \{(m, a) \mid m \in \mathbb{N}, a \in K_n\}.$$

(To be clear, one may think of this as an appropriate subset of $\mathbb{N} \times K_1 \times K_2 \times \cdots$.) Define an equivalence relation $\sim$ on A by: $(m, a) \sim (n, b)$ when either (1) $m \leqslant n$ and $b = f_{m,n}(a)$, or (2) $m \geqslant n$ and $a = f_{n,m}(b)$. Check that this is an equivalence relation on A. Set $K = A/\sim$, that is, K is the set of equivalence classes under $\sim$. For each $(m, a) \in A$, denote the corresponding equivalence class $[m, a] \in K$.

For each $i \geqslant 1$, define $g_i \colon K_i \to K$ as $g_i(a) = [i, a]$. We show that g_i is 1-1. Let $a, b \in K_i$ such that $g_i(a) = g_i(b)$. Then $[i, a] = [i, b]$, and so $(i, a) \sim (i, b)$. This means $b = f_{i,i}(a) = \mathrm{id}_{K_i}(a) = a$.

For $(m, a), (n, b) \in K$ define

$$(m, a) + (n, b) = \begin{cases} (n, f_{m,n}(a) + b) & \text{if } n \geqslant m \\ (m, a + f_{n,m}(b)) & \text{if } n \leqslant m. \end{cases}$$

Note that $(m, a)+(n, b) = (n, b)+(m, a)$. Fix elements $(m, a), (m', a'), (n, b), (n', b') \in A$ such that $(m, a) \sim (m', a')$ and $(n, b) \sim (n', b')$.

Claim: $(m, a) + (n, b) \sim (m', a') + (n', b')$. To this end, we show that $(m, a) + (n, b) \sim (m', a') + (n, b)$. (A similar argument then shows that $(m', a') + (n, b) \sim (m', a') + (n', b')$, and hence the claim.) Assume that $m \leqslant m'$. By definition of $\sim$, this implies $a' = f_{m,m'}(a)$. Consider three cases:

Case 1: $n \leqslant m \leqslant m'$.

$$\begin{aligned} (m, a) + (n, b) &= (m, a + f_{n,m}(b)) \\ &\sim (m', f_{m,m'}(a + f_{n,m}(b)) \\ &= (m', f_{m,m'}(a) + f_{m,m'}(f_{n,m}(b))) \\ &= (m', a' + f_{n,m'}(b)) \\ &= (m', a') + (n, b) \end{aligned}$$

The other two cases ($m \leqslant n \leqslant m'$ and $m \leqslant m' \leqslant n$) are handled similarly.

For $[m, a], [n, b] \in K$ define

$$[m, a] + [n, b] = \begin{cases} [n, f_{m,n}(a) + b] & \text{if } n \geqslant m \\ [m, a + f_{n,m}(b)] & \text{if } n \leqslant m \end{cases}$$

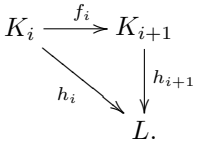
$$[m, a][n, b] = \begin{cases} [n, f_{m,n}(a)b] & \text{if } n \geqslant m \\ [m, af_{n,m}(b)] & \text{if } n \leqslant m. \end{cases}$$

The above claim shows that this addition is well-defined. A similar argument shows that this multiplication is well-defined. Check that the element $[1, 0] \in K$ is an additive identity. Check that the element $[1, 1] \in K$ is a multiplicative identity. Since g_1 is 1-1, we know that $[1, 0] \neq [1, 1]$ in K. Check that, for each $[m, a] \in K$, the element $[m, -a] \in K$ is an additive inverse for $[m, a]$ in K. Check that, for

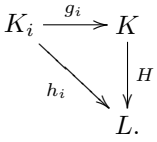
each $[m, a] \in K$ with $a \neq 0$, the element $[m, a^{-1}] \in K$ is a multiplicative inverse for $[m, a]$ in K. (Since g_m is 1-1, we know that $[m, a] \neq [m, 0] = [1, 0]$ in K.) Check that K is a field.

Check that each map $g_i \colon K_i \to K$ is a homomorphism of fields. Check that $g_{i+1} f_i = g_i$ for each $i \geqslant 1$. This shows that condition (1) is satisfied.

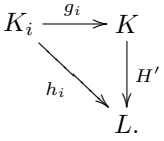
For condition (2), let L be a field with homomorphisms of fields $h_i \colon K_i \to L$ such that, for each $i \geqslant 1$, the following diagram commutes



Define $h \colon A \to L$ by the formula $h(m, a) = h_m(a)$. Check that, when $(m, a) \sim (n, b)$, we have $h(m, a) = h(n, b)$. It follows that the function $H \colon K \to L$ given by the formula $H([m, a]) = h(m, a) = h_m(a)$ is well-defined. Check that H is a homomorphism of fields making each of the following diagrams commute:



For the uniqueness of H, suppose that $H' \colon K \to L$ is another homomorphism of fields making each of the following diagrams commute:



For each $[m, a] \in K$, it follows that

$$H'([m, a]) = H'(g_m(a)) = h_m(a) = H([m, a])$$

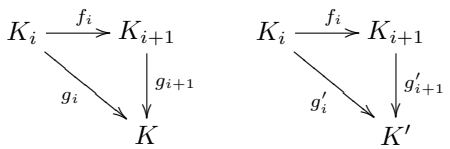
and so $H' = H$. □

8. Day 8

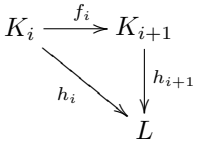
Here is a uniqueness statement for the previous result.

PROPOSITION 8.1. *Let $K_1, K_2, \ldots$ be fields, and for $i \geqslant 1$ let $f_i \colon K_i \to K_{i+1}$ be a homomorphism of fields. Let K and K' be fields with homomorphisms of fields $g_i \colon K_i \to K$ and $g'_i \colon K_i \to K'$ satisfying conditions* (1) *and* (2) *from Proposition 7.1. That is, assume that*

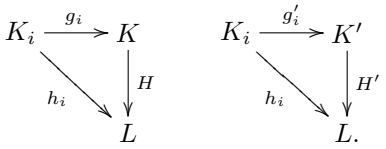
(1) *for each $i \geqslant 1$, the following diagrams commute*



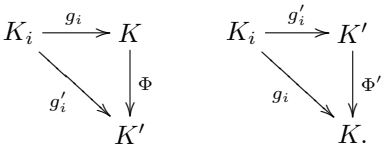
(2) *for each field L with homomorphisms of fields $h_i\colon K_i \to L$ such that, for each $i \geqslant 1$, the following diagram commutes*



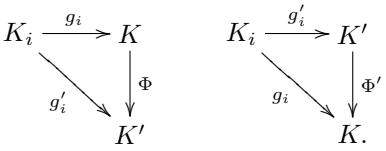
there exists unique homomorphisms of fields $H\colon K \to L$ and $H'\colon K' \to L$ making each of the following diagrams commute:



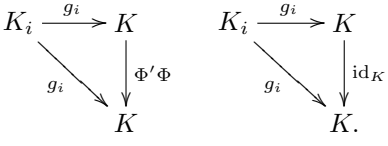
Then there are isomorphisms of fields $\Phi\colon K \to K'$ and $\Phi'\colon K' \to K$ making each of the following diagrams commute:



Proof. Conditions (1) and (2) provide homomorphisms of fields $\Phi\colon K \to K'$ and $\Phi'\colon K' \to K$ making each of the following diagrams commute:



We need to show that Φ and Φ' are isomorphisms. The above diagrams combine to provide the first commutative diagram in the next display



Since the second diagram also commutes, the uniqueness condition in (2) implies that $\Phi'\Phi = \mathrm{id}_K$. A similar argument shows that $\Phi\Phi' = \mathrm{id}_K$. Hence Φ and Φ' are isomorphisms. □

Proposition 8.2. *Let $K_1, K_2, \ldots$ be fields, and for $i \geqslant 1$ let $f_i\colon K_i \to K_{i+1}$ be a homomorphism of fields. Let K be a field with homomorphisms of fields $g_i\colon K_i \to K$ satisfying conditions* (1) *and* (2) *from Proposition 7.1. Then $\cup_i(\mathrm{Im}(g_i)) = K$. In other words, for each $a \in K$, there exists $i \geqslant 1$ and $a_i \in K_i$ such that $a = g_i(a_i)$.*

Proof. Exercise. Show that $K' = \cup_i \mathrm{Im}(g_i)$ is a subfield of K, and that there are homomorphisms of fields $g_i'\colon K_i \to K'$ that satisfy conditions (1) and (2) from

Proposition 7.1. Then argue as in the proof of Proposition 8.1 to show that the inclusion $K' \subseteq K$ must be an isomorphism. □

THEOREM 8.3. *Let K be a field. TFAE:*

(i) *Every polynomial $f \in k[x]$ with positive degree has a root in k;*
(ii) *Every polynomial $f \in k[x]$ with positive degree splits into linear factors in $k[x]$;*
(iii) *If $k \subseteq K$ is an algebraic extension, then $k = K$.*

PROOF. (i) $\implies$ (ii) Let $f \in k[x]$ with $\deg(f) \geqslant 1$. By assumption, f has a root $a \in k$, and so $f = (x-a)g$ for some $g \in k[x]$. Note that $\deg(g) = \deg(f) - 1$, so an induction argument shows that f splits into linear factors in $k[x]$.

(ii) $\implies$ (iii) Let $k \subseteq K$ be an algebraic extension. Let $u \in K$, which is necessarily algebraic over k. Let $f \in k[x]$ be the minimal polynomial of u over k. By assumption, f splits into linear factors in $k[x]$. However, f is irreducible by assumption, and so f is linear. Since f is monic, it is of the form $f = x - v$ for some $v \in k$. Since u is a root of $f = x - v$, we have $u = v \in k$. Thus, we have $K \subseteq k \subseteq K$ and so $k = K$.

(iii) $\implies$ (i) Let $f \in k[x]$ with $\deg(f) \geqslant 1$. Theorem 5.5 yields a field extension $k \subseteq k(u)$ such that u is a root of f. Theorem 6.2 implies that this extension is algebraic, so our assumption implies $k = k(u)$. Hence, $u \in k$ is a root of f. □

DEFINITION 8.4. A field k is *algebraically closed* if it satisfies the equivalent conditions of Theorem 8.3. If $k \subseteq K$ is an algebraic field extension such that K is algebraically closed, then K is an *algebraic closure of k*.

9. Day 9

It is time to start being precise.

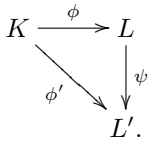
DEFINITION 9.1. Fix a homomorphism of commutative rings with identity $\phi\colon R \to S$, let $\hat{\phi}\colon R[x] \to S[x]$ denote the homomorphism of polynomial rings given by $\hat{\phi}(\sum_i a_i x^i) = \sum_i \phi(a_i) x^i$. An element $a \in S$ is a *root* of $f \in R[x]$ if a is a root of $\hat{\phi}(f) \in S[x]$.

We say that S is *generated as an R-algebra by a set $X \subseteq S$* if $S = \mathrm{Im}(\phi)[X]$.

DEFINITION 9.2. A *field extension* is a homomorphism of fields $\phi\colon K \to L$. Note that ϕ is a monomorphism, and so $K \cong \mathrm{Im}(\phi) \subseteq L$.

A field extension $\phi\colon K \to L$ is *algebraic* if $\mathrm{Im}(\phi) \subseteq L$ is algebraic; it is *transcendental* if $\mathrm{Im}(\phi) \subseteq L$ is transcendental; the field L is *generated as a field over K by a set $X \subseteq L$* if $L = \mathrm{Im}(\phi)(X)$.

Let $\phi\colon K \to L$ and $\phi'\colon K \to L'$ be field extensions. A map $\psi\colon L \to L'$ is a *K-homomorphism of fields* if it is a homomorphism of fields making the following diagram commute:

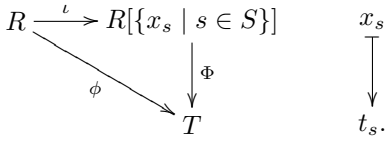


DEFINITION 9.3. If $\phi\colon K \to L$ is an algebraic field extension such that K is algebraically closed, then L is an *algebraic closure of K*.

We will show below that every field has an algebraic closure. First we need another tool: polynomial rings in infinitely many variables.

REMARK 9.4. Let R be a commutative ring with identity and let S be a set. There exists a ring $P = R[\{x_s \mid s \in S\}]$ of polynomials where the set of variables $\{x_s \mid s \in S\}$ is in bijection with S. Every element of $R[\{x_s \mid s \in S\}]$ is of the form $f(x_{s_1}, x_{s_2}, \ldots, x_{s_n})$ for some polynomial $f \in R[y_1, \ldots, y_n]$, that is, of the form $\sum_{i_1,\ldots,i_n \in \mathbb{N}}^{\text{finite}} a_{i_1,\ldots,i_n} x_{s_1}^{i_1} \cdots x_{s_n}^{i_n}$ for some $a_{i_1,\ldots,i_n} \in R$. Furthermore, the set of monomials $\{x_{s_1}^{i_1} \cdots x_{s_n}^{i_n} \mid s_1, \ldots, s_n \in S; i_1, \ldots, i_n \in \mathbb{N}\}$ is linearly independent, i.e., forms a basis for $R[\{x_s \mid s \in S\}]$ as an R-module. Addition and multiplication are defined in the natural way. If S is finite, then $R[\{x_s \mid s \in S\}] \cong R[x_1, \ldots, x_n]$ where $n = |S|$. The inclusion of constant polynomials defines a monomorphism of commutative rings with identity $\iota\colon R \to R[\{x_s \mid s \in S\}]$.

The ring P has the following universal mapping property: Let $\phi\colon R \to T$ be a homomorphism of commutative rings with identity. For each subset $\{t_s \in T \mid s \in S\}$ there exists a unique homomorphism of commutative rings with identity $\Phi\colon R[\{x_s \mid s \in S\}] \to T$ such that $\Phi(x_s) = t_t$ for each $s \in S$ and $\Phi(a) = a$ for all $a \in R$, that is, such that the following diagram commutes:



See Hungerford, Exercise III.5.4 for details of the construction.

LEMMA 9.5. *Let K be a field. There is an algebraic field extension $\phi\colon K \to K'$ such that, for every polynomial $f \in K[x]$ of positive degree, the field K' contains a root of f.*

PROOF. Let $S = \{f \in K[x] \mid \deg(f) \geqslant 1\}$. Let X denote a set of variables, indexed by the set S. For each $f \in S$, let $x_f \in X$ denote the variable in X corresponding to f. Consider the polynomial ring $K[X] = K[\{x_f \mid f \in S\}]$, and let

$$I = (\{f(x_f) \mid f \in S\}) \subseteq K[X]$$

which is an ideal in $K[X]$. Note that the coset $x_f + I \in K[X]/I$ is a root of f.

Claim: $1 \notin I$. Suppose that $1 \in I$. then there exist polynomials $f_1, \ldots, f_n \in S$ and $g_1, \ldots, g_n \in K[X]$ such that $1 = \sum_i g_i f(x_{f_i})$. By Theorem 6.10, there is a field extension $\alpha\colon K \to L$ such that each f_i has a root $a_i \in L$. Remark 9.4 yields a homomorphism of commutative rings with identity $\psi\colon K[X] \to L$ such that $\psi(x_{f_i}) = a_i$ for $i = 1, \ldots, n$ and $\psi(x_f) = 0$ for $f \neq f_i$. In particular, we have $\psi(1) = 1 \neq 0$. However, we have

$$1 = \psi(1) = \psi(\textstyle\sum_i g_i f(x_{f_i})) = \sum_i \psi(g_i)\psi(f(x_{f_i})) = \sum_i \psi(g_i) f(a_i) = \sum_i \psi(g_i) 0 = 0$$

a contradiction. This establishes the claim.

The claim implies that $I \subsetneq K[X]$, and so there is a maximal ideal $\mathfrak{m} \subset K[X]$ such that $I \subseteq \mathfrak{m}$. Since $x_f + I \in K[X]/I$ is a root of f in $K[X]/I$ and $I \subseteq \mathfrak{m}$, it follows that $x_f + \mathfrak{m} \in K[X]/\mathfrak{m}$ is a root of f in the field $K' = K[X]/\mathfrak{m}$. Let $\phi\colon K \to K'$ denote the composition $K \to K[X] \to K[X]/\mathfrak{m} = K'$. Note that K' is generated as a K-algebra (and therefore as a field extension of K) by the set $\{x_f + \mathfrak{m} \mid f \in S\}$. Since every element of this set is algebraic, it follows that the

extension $K \to K'$ is algebraic, and that every polynomial in S has a root in K'. That is, the homomorphism ϕ has the desired properties. □

10. Day 10

THEOREM 10.1. *Every field K has an algebraic closure.*

PROOF. Set $K_1 = K$. Lemma 9.5 provides a homomorphism of fields $\phi_1 \colon K_1 \to K_2$ such that the extension $\operatorname{Im}(\phi_1) \subseteq K_2$ is algebraic and for every polynomial $f \in K_1[x]$ of positive degree, the field K_2 contains a root of $\hat{\phi}_1(f)$. Inductively, for each $i \geqslant 1$ there is a homomorphism of fields $\phi_i \colon K_i \to K_{i+1}$ such that the extension $\operatorname{Im}(\phi_i) \subseteq K_{i+1}$ is algebraic and for every polynomial $f \in K_i[x]$ of positive degree, the field K_{i+1} contains a root of $\hat{\phi}_i(f)$.

Propositions 7.1 and 8.2 say that there exists a field $\overline{K}$ with homomorphisms of fields $g_i \colon K_i \to \overline{K}$ satisfying the following properties:

(1) For each $i \geqslant 1$, the following diagram commutes

$$\begin{array}{ccc} K_i & \xrightarrow{\phi_i} & K_{i+1} \\ & \searrow^{g_i} & \downarrow{\scriptstyle g_{i+1}} \\ & & \overline{K}. \end{array}$$

(2) For each $a \in \overline{K}$, there exists $i \geqslant 1$ and $a_i \in K_i$ such that $a = g_i(a_i)$.

For integers $j \geqslant i \geqslant 1$, define $\phi_{i,j} \colon K_i \to K_j$ as

$$\phi_{i,j} = \begin{cases} \mathrm{id}_{K_i} \colon K_i \to K_i & \text{if } j = i \\ \phi_i \colon K_i \to K_{i+1} & \text{if } j = i+1 \\ \phi_{j-1} \circ \cdots \circ \phi_{i+1} \circ \phi_i \colon K_i \to K_j & \text{if } j > i+1. \end{cases}$$

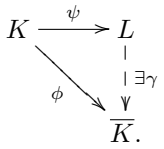
Claim: $\overline{K}$ is algebraically closed. Let $f = \sum_{i=0}^{d} b_i x^i \in \overline{K}[x]$ be a polynomial with $\deg(f) \geqslant 1$. We will show that f has a root in $\overline{K}$. Condition (2) implies that, for $i = 0, \dots, d$ there exists j_i and $c_i \in K_{j_i}$ such that $b_i = g_{j_i}(c_i)$. Let $j = \max\{j_0, \dots, j_d\}$. For $i = 0, \dots, d$ set $u_i = \phi_{j_i,j}(c_i)$. Condition (1) implies that $b_i = g_j(u_i)$ for each i. Set $\tilde{f} = \sum_{i=0}^{d} u_i x^i \in \overline{K}_j[x]$. This is a polynomial with $\deg(\tilde{f}) = \deg(f) \geqslant 1$ and $\hat{g}_j(\tilde{f}) = f$. By construction, the field K_{j+1} contains a root v of $\tilde{f}$. It follows that the element $g_{j+1}(v) \in \overline{K}$ is a root of f.

Claim: $\overline{K}$ is an algebraic closure for $K = K_1$. Because of the previous claim, it suffices to show that the extension $g_1 \colon K_1 \to \overline{K}$ is algebraic. Let $u \in \overline{K}$. Condition (2) implies that there exists $i \geqslant 1$ and $v \in K_i$ such that $u = g_i(v)$. Since K_j is algebraic over K_{j-1} for each $j \geqslant 2$, an induction argument using Theorem 6.3 shows that each K_j is algebraic over $K_1 = K$. Thus, the element $v \in K_i$ is algebraic over K_1, and it follows that u is also algebraic over K_1. □

Here is a "universal mapping property" for algebraic closures. Note that we do not claim that the map γ in this result is unique.

THEOREM 10.2. *Let K be a field. Let $\phi \colon K \to \overline{K}$ be an algebraic closure of K, and let $\psi \colon K \to L$ be an algebraic field extension. Then there is a K-homomorphism*

of fields $\gamma\colon L \to \overline{K}$, that is, there is a homomorphism of fields $\gamma\colon L \to \overline{K}$ making the following diagram commute



PROOF. Case 1: We have $K \subseteq L$ where ϕ is the inclusion. Let Σ denote the set of all ordered pairs (F, α) such that K is an intermediate field of K and L and such that $\alpha\colon F \to \overline{K}$ is a K-homomorphism of fields. Partially order Σ as follows: $(F, \alpha) \leqslant (F', \alpha')$ when $F \subseteq F'$ and $\alpha'|_F = \alpha$. Verify that this is a partial order on Σ. Note that $\Sigma \neq \emptyset$ because $(K, \phi) \in \Sigma$.

Claim: Σ contains a maximal element (K', ϕ'). To show this, we show that Σ satisfies the hypotheses of Zorn's Lemma. Let $\mathcal{C}$ be a chain in Σ. Then each element of $\mathcal{C}$ is an ordered pair (F, α). In particular, the set $\mathcal{C}' = \{F \mid (F, \alpha) \in \mathcal{C} \text{ for some } \alpha\}$ is a chain of intermediate fields of K and L. It follows from an exercise that $E = \cup_{(F,\alpha)\in\mathcal{C}} F$ is an intermediate field of K and L.

Define a function $\beta\colon E \to \overline{K}$ as follows. For $e \in E$, we have $e \in F$ for some $(F, \alpha) \in \mathcal{C}$, so we set $\beta(e) = \alpha(e)$. To see that this is well-defined, suppose that $e \in F'$ for some $(F', \alpha') \in \mathcal{C}$. We need to show that $\alpha(e) = \alpha'(e)$. Since $\mathcal{C}$ is a chain, we have either $(F, \alpha) \leqslant (F', \alpha')$ or $(F', \alpha') \leqslant (F, \alpha)$. By symmetry, assume that $(F, \alpha) \leqslant (F', \alpha')$. By definition, this entails $F \subseteq F'$ and $\alpha'|_F = \alpha$. It follows that $\alpha(e) = \alpha'|_F(e) = \alpha'(e)$, as desired.

Since each map α is a K-homomorphism of fields, it is straightforward to show that $\beta\colon E \to \overline{K}$ is a K-homomorphism of fields. Hence $(E, \beta) \in \Sigma$. Furthermore, by construction, if $(F, \alpha) \in \mathcal{C}$, then $F \subseteq E$ and $\beta\,|_F = \alpha$: hence, $(F, \alpha) \leqslant (E, \beta)$. That is, (E, β) is an upper bound for $\mathcal{C}$ in Σ. Thus, Σ satisfies the hypotheses of Zorn's Lemma, and so Σ contains a maximal element (K', ϕ').

Claim: $K' = L$. (Once we show this, we will be done since then $\phi'\colon L \to \overline{K}$ will satisfy the desired conclusions.) Suppose $K' \neq L$, that is $K' \subsetneq L$, and let $u \in L - K'$. Since L is algebraic over K and $K \subseteq K' \subset L$, we know that u is algebraic over K'. We will show that there is a K-homomorphism of fields $\gamma\colon K'(u) \to \overline{K}$ such that $\gamma\,|_{K'} = \phi'$. This will contradict the maximality of (K', ϕ') in Σ, thus completing the proof in this case.

Let $f \in K'[x]$ be the minimal polynomial of u. Since $\phi'\colon K' \to \overline{K}$ is a field extension and $\overline{K}$ is algebraically closed, we know that $\overline{K}$ contains a root v of f. Theorem 5.2 provides an isomorphism $\delta\colon K'(u) \to \mathrm{Im}(\phi')(v)$ such that $\delta\,|_{K'} = \phi'$. In particular, this is a K-homomorphism such that $\delta\,|_{K'} = \phi'$. Letting γ be the composition of δ with the natural injection $\mathrm{Im}(\phi')(v) \subseteq \overline{K}$, we have the desired map.

Case 2: The general case. Let $K_1 = \mathrm{Im}(\psi) \subseteq L$. This is an algebraic extension, so Case 1 provides a K-homomorphism $\gamma_1\colon K_1 \to \overline{K}$. Letting γ be the composition of γ_1 with the isomorphism $K \to \mathrm{Im}(\psi) = K_1$ induced by ψ, we have the desired map. □

11. Day 11

We put the words "universal mapping property" in quotes because the map γ may not be unique, as the following example shows.

EXAMPLE 11.1. We shall see that $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$ via the natural inclusion $\mathbb{R} \subset \mathbb{C}$. With $L = \mathbb{C} = \overline{K}$ in the previous result, there are two $\mathbb{R}$-isomorphisms $\gamma\colon \mathbb{C} \to \mathbb{C}$, namely, the identity and complex conjugation. See Example 5.4.

In spite of the lack of uniqueness, we show below that the algebraic closure of a field K is unique up to K-isomorphism. First, some preliminaries.

LEMMA 11.2. *Let K be a field, and let $\phi\colon K \to L$ and $\phi'\colon K \to L'$ be algebraic field extensions. Let $\psi\colon L \to L'$ be a K-homomorphism. For each $u \in L$ with minimal polynomial $f \in K[x]$, the element $\psi(u) \in L'$ is a root of f.*

PROOF. Write $f = \sum_i a_i x^i$. If we think of K as a subfield of L and L', then we have

$$f(\psi(u)) = \textstyle\sum_i a_i \psi(u)^i = \psi(\sum_i a_i u^i) = \psi(f(u)) = \psi(0) = 0.$$

If we remember the homomorphisms, then we write

$$f(\psi(u)) = \textstyle\sum_i \phi'(a_i)\psi(u)^i = \sum_i \psi(\phi(a_i))\psi(u)^i = \psi(\sum_i \phi(a_i)u^i) = \psi(f(u)) = \psi(0) = 0.$$

□

THEOREM 11.3. *Let K be a field, and let $\phi\colon K \to L$ be an algebraic extension. If $\psi\colon L \to L$ is a K-homomorphism, then ψ is an isomorphism.*

PROOF. We know that ψ is injective, so it remains to show that ψ is surjective. Let $u \in L$ with minimal polynomial $f \in K[x]$. Let $u = u_1, \ldots, u_n \in L$ be the distinct roots of f in L. Lemma 11.2 implies that, for each i, there is a j such that $\psi(u_i) = u_j$. In other words, ψ restricts to a function $\psi'\colon \{u_1, \ldots, u_n\} \to \{u_1, \ldots, u_n\}$. Since ψ is 1-1, the same is true of ψ'. Hence, the Pigeonhole Principle implies that ψ' is onto. Hence, there is a j such that $\psi(u_j) = u_1 = u$. Thus ψ is onto. □

The next example shows that the conclusion of the previous result fails if L is not algebraic over K.

EXAMPLE 11.4. Let k be a field and let $k(x)$ be the field of rational functions over k in one variable. Theorem 5.1 provides a k-homomorphism $\phi\colon k(x) \to k(x)$ such that $\phi(x) = x^2$. A homework exercise shows that this is not an isomorphism.

THEOREM 11.5. *Let K be a field, and let $\phi\colon K \to L$ and $\phi'\colon K \to L'$ be algebraic closures. There is a K-isomorphism $\psi\colon L \xrightarrow{\cong} L'$. Every K-homomorphism $\psi\colon L \xrightarrow{\cong} L'$ is an isomorphism.*

PROOF. Theorem 10.2 provides K-homomorphisms $\psi\colon L \to L'$ and $\psi'\colon L' \to L$. The composition $\psi\psi'\colon L' \to L'$ is a K-homomorphism. Since the extension $\phi\colon K \to L$ is algebraic, Theorem 11.3 implies that $\psi\psi'$ is bijective. It follows that ψ is onto. Since we already know that ψ is 1-1, we conclude that it is an isomorphism. □

Now we start counting K-homomorphisms $L \to \overline{K}$.

LEMMA 11.6. *Let $\phi\colon K \to K(u)$ be a finite simple field extension, and let $\psi\colon K \to \overline{K}$ be an algebraic closure. If $\alpha, \alpha'\colon K(u) \to \overline{K}$ are K-homomorphisms such that $\alpha(u) = \alpha'(u)$, then $\alpha = \alpha'$.*

PROOF. We have $K(u) = K[u]$ by Theorem 3.7(a), and Theorem 4.1(b) implies $\{1, u, u^2, \dots, u^{n-1}\}$ is a K-basis for $K(u)$ where $n = [K(u) : K]$.

First, we think of K as a subfield of $K(u)$ and $\overline{K}$. For each $\sum_i a_i u^i \in K(u)$, our assumptions imply

$$\alpha'(\textstyle\sum_i a_i u^i) = \sum_i a_i \alpha'(u)^i = \sum_i a_i \alpha(u)^i = \alpha'(\sum_i a_i u^i)$$

and so $\alpha' = \alpha$.

When we remember the homomorphisms, an arbitrary element of $K(u)$ has the form $\sum_i \phi(a_i)u^i$ with the $a_i \in K$, and we have

$$\begin{aligned}\alpha'(\textstyle\sum_i \phi(a_i)u^i) &= \sum_i \alpha'(\phi(a_i))\alpha'(u)^i = \sum_i \psi(a_i)\alpha'(u)^i = \sum_i \psi(a_i)\alpha(u)^i \\ &= \sum_i \alpha(\phi(a_i))\alpha(u)^i = \alpha'(\textstyle\sum_i \phi(a_i)u^i)\end{aligned}$$

and so $\alpha' = \alpha$. □

LEMMA 11.7. *Let $\phi\colon K \to K(u)$ be a simple finite field extension, and let $\psi\colon K \to \overline{K}$ be an algebraic extension. The number of K-homomorphisms $K(u) \to \overline{K}$ is equal to the number of distinct roots of u in $\overline{K}$, and this is at most $[K(u) : K]$.*

PROOF. Let $S = \{K\text{-homomorphisms } K(u) \to \overline{K}\}$. Let $f \in K[x]$ be the minimal polynomial for u, and let $u_1, \dots, u_m \in \overline{K}$ be the distinct roots of f in $\overline{K}$. We show that $|S| = m$. It then follows that $|S| = m \leqslant \deg(f) = [K(u) : K]$.

For $i = 1, \dots, m$ there is a K-homomorphism $\alpha_i\colon K(u) \to K(u_i) \subseteq \overline{K}$ such that $\alpha_i(u) = u_i$. Since $u_i \neq u_j$ when $i \neq j$, we have m distinct K-homomorphisms, and so $|S| \geqslant m$.

On the other hand, let $\alpha\colon K(u) \to \overline{K}$ be a K-homomorphism. Lemma 11.2 implies that $\alpha(u)$ is a root of f, and so $\alpha(u) = u_i$ for some i. Lemma 11.6 implies that α is unique with this property, and so $|S| \leqslant m$. □

LEMMA 11.8. *Let $\psi\colon K \to \overline{K}$ and $\phi\colon K \to L$ and $\rho\colon L \to M$ be field extensions. Let T denote the set of ordered pairs (α, β) such that $\alpha\colon L \to \overline{K}$ is a K-homomorphism, and $\beta\colon M \to \overline{K}$ is an L-homomorphism where the L-algebra structure for $\overline{K}$ is determined by α. Then T is in bijection with the set of K-homomorphisms $M \to \overline{K}$.*

PROOF. Identify L with its image in M, and identify K with its image in $L \subseteq M$. Let $S = \{K\text{-homomorphisms } M \to \overline{K}\}$. We construct bijections $S \leftrightarrow T$.

To define $\Phi\colon T \to S$, let $(\alpha, \beta) \in T$. So $\alpha\colon L \to \overline{K}$ and $\beta\colon M \to \overline{K}$ are such that $\alpha\phi = \psi$ and $\beta\rho = \alpha$, i.e., such that $\psi = \alpha|_K$ and $\alpha = \beta|_L$. It follows that $\beta|_K = \beta|_L|_K = \alpha|_K$, and so β is a K-homomorphism. That is, we may define $\Phi(\alpha, \beta) = \beta$.

To define $\Psi\colon S \to T$, let $\gamma\colon M \to \overline{K}$ be a K-homomorphism. It follows that $\gamma|_L\colon L \to \overline{K}$ is a K-homomrophism, and so we can define $\Psi(\gamma) = (\gamma|_L, \gamma)$. Check that Φ and Ψ are inverses and hence bijections. □

12. Day 12

THEOREM 12.1. *Let $\phi\colon K \to L$ be a field extension with $n = [L : K] < \infty$, and let $\psi\colon K \to \overline{K}$ be an algebraic closure. The number of K-homomorphisms $L \to \overline{K}$ is at most n.*

PROOF. Write $L = K(u_1, \ldots, u_m)$. We proceed by induction on m. The base case $m = 1$ is in Lemma 11.7.

For the induction step, assume that $m > 1$ and write

$$L = K(u_1, \ldots, u_m) = K(u_1, \ldots, u_{m-1})(u_m).$$

Lemma 11.8 implies that every K-homomorphism $\beta\colon K(u_1, \ldots, u_m) \to \overline{K}$ is uniquely obtained from the following procedure:

(1) Choose a K-homomorphism $\alpha\colon K(u_1, \ldots, u_{m-1}) \to \overline{K}$ (there are at most $[K(u_1, \ldots, u_{m-1}) : K]$ many choices by induction);
(2) Choose a $K(u_1, \ldots, u_{m-1})$-homomorphism $\beta\colon K(u_1, \ldots, u_{m-1})(u_m) \to \overline{K}$ (there are at most $[K(u_1, \ldots, u_m) : K(u_1, \ldots, u_{m-1})]$ many choices for β (for each choice of α)).

It follows that the total number of choices for β is at most

$$\begin{aligned}[K(u_1, \ldots, u_{m-1}) : K][K(u_1, \ldots, u_m) : K(u_1, \ldots, u_{m-1})] &= [K(u_1, \ldots, u_m) : K] \\ &= [L : K]\end{aligned}$$

by the Tower Law. □

COROLLARY 12.2. *Let $\phi\colon K \to L$ be a finite field extension, and let $K \to \overline{K}$ be an algebraic closure. Fix a K-homomorphism $L \to \overline{K}$ and identify L with its image in $\overline{K}$. Then*

$$|\{K\text{-homomorphisms } L \to L\}| \leqslant |\{K\text{-homomorphisms } L \to \overline{K}\}| \leqslant [L : K]$$

where $K \to \overline{K}$ is an algebraic closure. Furthermore, the first inequality is an equality if and only if, for all K-homomorphisms $\rho\colon L \to \overline{K}$, we have $\mathrm{Im}(\rho) = L$.

PROOF. Each K-homomorphism $L \to L$ uniquely determines a K-homomorphism $L \to \overline{K}$ by composing with the inclusion $L \subseteq \overline{K}$. It follows that the number of K-homomorphisms $L \to L$ is at most the number of K-homomorphisms $L \to \overline{K}$, which is at most n by Theorem 12.1. This argument gives a 1-1 map $\{K\text{-homomorphisms } L \to L\} \hookrightarrow \{K\text{-homomorphisms } L \to \overline{K}\}$. Since these sets are finite, the map is a bijection if and only if the sets have the same cardinality. □

The next examples show that each inequality in the corollary can be strict.

EXAMPLE 12.3. We can have

$$|\{K\text{-homomorphisms } L \to \overline{K}\}| < [L : K].$$

Let $k = \mathbb{Z}/(2)$. Let $L = k(t)$ be the field of rational functions in one variable over $k = \mathbb{Z}/(2)$. Let $K = k(t^2) \subseteq k(t) = L$. Then $t \in k(t) - k(t^2)$, and so $[k(t) : k(t^2)] \geqslant 2$. On the other hand t is a root of the polynomial $x^2 - t^2 \in k(t^2)[x]$, and so $[k(t) : k(t^2)] \leqslant 2$. Hence, we have $[k(t) : k(t^2)] = 2$, that is $[L : K] = 2$.

We claim that there is only one K-homomorphism $L \to \overline{K}$. To see this, use the fact that $L = K(t)$ in Lemma 11.7 to see that the number of K-homomorphisms $L \to \overline{K}$ is the same as the number of distinct roots of $x^2 - t^2$ in $\overline{K}$. However, if $T \in \overline{K}$ is a root of $x^2 - t^2$, then we have $0 = T^2 - t^2$ and so

$$x^2 - t^2 = x^2 - T^2 = x^2 - 2Tx + T^2 = (x - T)^2.$$

Since $\overline{K}[x]$ is a UFD, it follows that the only root of $x^2 - t^2$ in $\overline{K}$ is T.

EXAMPLE 12.4. We can have

$$|\{K\text{-homomorphisms } L \to L\}| < |\{K\text{-homomorphisms } L \to \overline{K}\}|.$$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$. The irreducible polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $f = x^3 - 2$. The field L only contains one root of f, namely $\sqrt[3]{2}$. Let $K \subseteq \overline{K}$ be an algebraic closure such that $\overline{K} \subseteq \mathbb{C}$. Then $\overline{K}$ contains three distinct roots for f, namely $\sqrt[3]{2}$, $\sqrt[3]{2}e^{2\pi i/3} = \sqrt[3]{2}(-1+\sqrt{3}i)/2$, $\sqrt[3]{2}e^{4\pi i/3} = \sqrt[3]{2}(-1-\sqrt{3}i)/2$. Thus, we have

$$|\{K\text{-homomorphisms } L \to L\}| = 1 < 3 = |\{K\text{-homomorphisms } L \to \overline{K}\}|$$

by Lemma 11.7.

DEFINITION 12.5. Let $\phi\colon K \to L$ be a finite field extension. The *Galois group* of L over K is

$$\mathrm{Gal}(L:K) = \{K\text{-homomorphisms } L \to L\}.$$

This is a group under composition since each K-homomorphism $L \to L$ is an isomorphism.

The extension $\phi\colon K \to L$ is *Galois* if $|\mathrm{Gal}(L:K)| = [L:K]$.

The field L is a *splitting field* for a polynomial $f \in K[x]$ if f splits into linear factors in $L[x]$ and $L = K(u_1, \ldots, u_n)$ where $u_1, \ldots, u_n$ are roots of f in L.

PROPOSITION 12.6. *Let $\phi\colon K \to L$ be a finite field extension, and let $\psi\colon K \to \overline{K}$ be an algebraic closure. Fix a K-homomorphism $L \to \overline{K}$ and identify L with its image in $\overline{K}$. The extension $\phi\colon K \to L$ is Galois if and only if it satisfies the following conditions:*

1. *For each K-homomorphisms $\rho\colon L \to \overline{K}$, we have $\mathrm{Im}(\rho) = L$; and*
2. *The number of K-homomorphisms $\rho\colon L \to \overline{K}$ is exactly $[L:K]$.*

PROOF. Corollary 12.2 says that condition (1) is equivalent to the condition

$$|\{K\text{-homomorphisms } L \to L\}| = |\{K\text{-homomorphisms } L \to \overline{K}\}|.$$

Condition (2) is exactly the equality

$$|\{K\text{-homomorphisms } L \to \overline{K}\}| = [L:K].$$

Thus, the result follows from the inequalities in Corollary 12.2. □

REMARK 12.7. Examples 12.3 and 12.4 show how each condition in Proposition 12.6 can fail.

13. Day 13

The next result analyzes condition (1) from Proposition 12.6.

THEOREM 13.1. *Let $\phi\colon K \to L$ be a finite field extension, and let $\psi\colon K \to \overline{K}$ be an algebraic closure. Fix a K-homomorphism $L \to \overline{K}$ and identify L with its image in $\overline{K}$. The following conditions are equivalent:*

- (i) *For each K-homomorphisms $\rho\colon L \to \overline{K}$, we have $\mathrm{Im}(\rho) = L$;*
- (ii) *For each K-homomorphisms $\rho\colon L \to \overline{K}$, we have $\mathrm{Im}(\rho) \subseteq L$;*
- (iii) *Every irreducible polynomial over K with a root in L splits into linear factors in $L[x]$;*
- (iv) *L is a splitting field for some polynomial $f \in K[x]$.*

PROOF. (i) $\implies$ (ii). Straightforward.

(ii) $\implies$ (i). By Theorem 11.3: since $K \to L$ is algebraic and ρ describes a K-homomorphism $L \to L$, we know that ρ maps onto L.

(ii) $\implies$ (iii). Let $f \in K[x]$ be irreducible and let $u_1, \ldots, u_n$ be the roots of f in $\overline{K}$. Assume that $u_1 \in L$. It suffices to show that each $u_i \in L$. Let $\phi_i \colon K(u_1) \to \overline{K}$ be a K-homomorphism such that $\phi_i(u_1) = u_i$. The extension $K \to L$ is finite, so the intermediate extension $K(u_1) \subseteq L$ is algebraic. Hence, Theorem 10.2 provides a $K(u_1)$-homomorphism $\psi_i \colon L \to \overline{K}$, that is, ψ_i is a K-homomorphism such that $\psi|_{K(u_1)} = \phi_i$. By assumption (ii), we have $u_i \in \mathrm{Im}(\phi_i) \subseteq \mathrm{Im}(\psi_i) \subseteq L$, as desired.

(iii) $\implies$ (iv). Since L is finite over K, we have $L = K(u_1, \ldots, u_n)$ for some $u_i \in L$. Let $f_i \in K[x]$ be the minimal polynomial for u_i and set $f = f_1 \cdots f_n$. Since each u_i is a root of f, it suffices to show that f splits into linear factors in $L[x]$. Since f_i is irreducible and has a root in L, condition (iii) says that f_i splits into linear factors in $L[x]$. Hence, the same is true for f.

(iv) $\implies$ (ii). Assume that L is a splitting field for $f \in K[x]$, and let $u_1, \ldots, u_n \in L$ be roots of f such that $L = K(u_1, \ldots, u_n)$. Let $\rho \colon L \to \overline{K}$ be a K-homomorphism. By assumption, f splits into linear factors in $L[x]$, and so L contains every root of f in $\overline{K}$. Thus, we assume that $u_1, \ldots, u_n$ is a complete list of the distinct roots of f in $\overline{K}$. Since $\rho(u_i) \in \overline{K}$ is a root of f, we have $\rho(u_i) \in L$ for each i.

Each element of L is of the form $\sum_i \sum_j a_{i,j} u_i^j$. The previous paragraph tells us $\rho(u_i) \in L$ for each i, and so

$$\rho\big(\textstyle\sum_i \sum_j a_{i,j} u_i^j\big) = \sum_i \sum_j a_{i,j} \rho(u_i)^j \in L.$$

Since this is so for an arbitrary element of L, we conclude that $\mathrm{Im}(\rho) \subseteq L$, as desired. □

DEFINITION 13.2. A finite field extension satisfying the equivalent conditions of Theorem 13.1 is a *normal* extension.

EXAMPLE 13.3. The example $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ from 12.4 is not normal because the polynomial $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible and has a root in $\mathbb{Q}(\sqrt[3]{2})$, but does not split into linear factors in $\mathbb{Q}(\sqrt[3]{2})[x]$.

EXAMPLE 13.4. Let $\phi \colon K \to L$ be a field extension with $[L : K] = 2$. We claim that this extension is normal. Identify K with its image in L. Since $[L : K] = 2$, we have $L = K(u)$ for each $u \in L - K$. The minimal polynomial $f \in K[x]$ of u has degree 2. Since $u \in L$ is a root of f, we have $f = (x - u)g$ for some $g \in L[x]$. Since $\deg(f) = 2$, we have $\deg(g) = 1$ and so $g = x - v \in L[x]$. That is, L contains the other root v of f. Thus, L is a splitting field for f over K, and so the extension is normal.

In particular, the extension $\mathbb{Z}/(2)(t^2) \subseteq \mathbb{Z}/(2)(t)$ from Example 12.3 is normal.

PROPOSITION 13.5. *Let K be a field and fix a polynomial $f \in K[x]$ of positive degree. Then f has a splitting field over K, and any two splitting fields of f are K-isomorphic.*

PROOF. Theorem 6.10 shows that there is a field extension $K \to L$ such that f splits into linear factors in $L[x]$. (The proof actually shows how to construct a splitting field.) To find a splitting field of f, let $u_1, \ldots, u_n$ be all the roots of f in L. Then the field $K(u_1, \ldots, u_n)$ is a splitting field of f.

Let $\phi\colon K \to L$ and $\phi'\colon K \to L'$ be splitting fields for f. Let $u_1, \ldots, u_n$ be all the roots of f in L. Let $h_1 \in K[x]$ be the minimal polynomial of u_1. Then $h_1 \big| f$ and so L' contains a root of h_1, call it $u_1' \in L'$. Theorem 5.2 provides a K-isomorphism $\psi_1\colon K(u_1) \to K(u_1')$. Inductively, for each i, there is a root $u_i' \in L$ of f and a K-isomorphism $\psi_i\colon K(u_1, \ldots, u_i) \to K(u_1', \ldots, u_i')$. Hence, there are roots of $u_1', \ldots, u_n' \in L'$ of f and a K-isomorphism $\psi_n\colon L = K(u_1, \ldots, u_n) \to K(u_1', \ldots, u_n') \subseteq L'$. This yields a K-homomorphism $\psi\colon L \to L'$. Similarly, we construct a K-homomorphism $\psi'\colon L' \to L$. Since L' is algebraic over K, the composition $\psi\psi'\colon L' \to L'$ is an isomorphism by Theorem 11.5. It follows that ψ is onto, and hence is an isomorphism. □

14. Day 14

Proposition 14.1. *Let K be a field and fix a polynomial $f \in K[x]$ of degree $n \geqslant 1$. If $\phi\colon K \to L$ is a splitting field of f, then $[L : K] \leqslant n!$.*

Proof. Let $u_1, \ldots, u_m$ be the distinct roots of f in L, and note that $m \leqslant n$. We have $[K(u_1) : K] \leqslant n$ because the minimal polynomial of u_1 in $K[x]$ divides f. We have $[K(u_1, u_2) : K(u_1)] \leqslant n - 1$ because the minimal polynomial of u_2 in $K(u_1)[x]$ divides $f/(x - u_1)$. Similarly, we have

$$[K(u_1, \ldots, u_i, u_{i+1}) : K(u_1, \ldots, u_i)] \leqslant n - i$$

for each i. Hence we have

$$\begin{aligned}[L : K] &= [K(u_1, \ldots, u_m) : K] = \textstyle\prod_{i=0}^{m-1} [K(u_1, \ldots, u_i, u_{i+1}) : K(u_1, \ldots, u_i)] \\ &\leqslant \textstyle\prod_{i=0}^{n-1} (n - i) = n!\end{aligned}$$

by the Tower Law. □

Definition 14.2. Let K be a field and let $\phi\colon \mathbb{Z} \to K$ be given by

$$\phi(n) = \begin{cases} \sum_{i=1}^{n} 1_K & \text{if } n \geqslant 1 \\ \sum_{i=1}^{|n|} -1_K & \text{if } n \leqslant 1 \\ 0_K & \text{if } n = 0. \end{cases}$$

Check that ϕ is a homomorphism of commutative rings with identity. It follows that $\operatorname{Ker}(\phi) \subset \mathbb{Z}$ is a prime ideal, and so $\operatorname{Ker}(\phi) = (n)$ for some integer $n \geqslant 0$, either 0 or prime. The number n is the *characteristic* of K, and we write $\operatorname{char}(K) = n$. We call ϕ the *characteristic function* for K.

Example 14.3. We have $\operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{C}) = 0$, and $\operatorname{char}(\mathbb{Z}/(p)) = p$ for each prime $p > 0$.

Exercise 14.4. Let K be a field.

(a) Show that $\operatorname{char}(K) = 0$ if and only if there is a homomorphism of fields $\mathbb{Q} \to K$.
(b) Show that $\operatorname{char}(K) = p > 0$ if and only if there is a homomorphism of fields $\mathbb{Z}/(p) \to K$.

Exercise 14.5. (Freshman dream) Let K be a field with $\operatorname{char}(K) = p > 0$. Show that, for all $a, b \in K$ we have $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ for each integer $n \geqslant 1$.

We next analyze condition (2) from Proposition 12.6.

THEOREM 14.6. *Let K be a field, and let $\psi\colon K \to \overline{K}$ be an algebraic closure. Identify K with its image in $\overline{K}$. Let $u \in \overline{K} - K$, and let $f \in K[x]$ be the minimal polynomial of u. The following conditions are equivalent:*

(i) $|\{K\text{-homomorphisms } \rho\colon K(u) \to \overline{K}\}| < [K(u) : K]$;
(ii) *f has a multiple (repeated) root in $\overline{K}$;*
(iii) $f' = 0$;
(iv) $\mathrm{char}(K) = p > 0$ *and there is an (irreducible, monic) polynomial $g \in K[x]$ such that $f = g(x^p)$;*
(v) $\mathrm{char}(K) = p > 0$ *and $(x-u)^p \big| f$ in $\overline{K}[x]$;*
(vi) *u is a multiple (repeated) root of f.*

PROOF. (i) $\iff$ (ii). Lemma 11.7 says that the number of K-homomorphisms $\rho\colon K(u) \to \overline{K}$ is equal to the the number of distinct roots of f in $\overline{K}$. Since f splits into linear factors in $\overline{K}[x]$, this number is less than $[K(u) : K] = \deg(f)$ if and only if f has a repeated root in $\overline{K}$.

(ii) $\implies$ (iii). Let $v \in \overline{K}$ be a repeated root of f. Proposition 3.11.12 implies that $f(v) = 0 = f'(v)$ where f' is the formal derivative of f. Suppose that $f' \neq 0$. It follows that $\deg(f') < \deg(f)$. Since f is monic and irreducible and has v as a root, we see that f is the minimal polynomial of v. Since v is a root of $f' \in K[x]$, it follows that $f \big| f'$. This implies $\deg(f) \leqslant \deg(f')$, a contradiction.

(iii) $\implies$ (iv). Let $d = \deg(f)$ and write $f = \sum_{i=0}^{d} a_i x^i$. Since f is monic, we have $a_d = 1$. Let $\phi\colon \mathbb{Z} \to K$ be the characteristic function for K.

Claim: $p = \mathrm{char}(K) > 0$ and, if $a_i \neq 0$, then $p \big| i$. We have $0 = f' = \sum_{i=1}^{d} i a_i x^{i-1}$. Since the elements $1, x, x_2, \ldots$ form a linearly independent set, it follows that each coefficient $ia_i = 0$. In other words, we have $\phi(i)a_i = 0$. When $i = d$, this says $0 = \phi(d)1 = \phi(d)$, and so $0 \neq d \in \mathrm{Ker}(\phi)$. This implies that $\mathrm{Ker}(\phi) \neq 0$, and so $\mathrm{char}(K) > 0$. Set $p = \mathrm{char}(K)$. If $a_i \neq 0$, then the equality $\phi(i)a_i = 0$ implies that $0 = a_i^{-1}\phi(i)a_i = \phi(i)$; hence, we have $i \in \mathrm{Ker}(\phi) = p\mathbb{Z}$ and so $p \big| i$.

It follows that we have

$$\begin{aligned} f &= a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d \\ &= a_0 + a_p x^p + a_{2p}x^{2p} + \cdots + a_{(e-1)p}x^{(e-1)p} + x^{ep} \\ &= a_0 + a_p (x^p)^1 + a_{2p}(x^p)^2 + \cdots + a_{(e-1)p}(x^p)^{e-1} + (x^p)^e. \end{aligned}$$

The polynomial $g = a_0 + a_p x^1 + a_{2p}x^2 + \cdots + a_{(e-1)p}x^{e-1} + x^e$, is monic, and the above display implies $f = g(x^p)$. Also g is irreducible: if $g = g_1 g_2$ with each $\deg(g_j) \geqslant 1$, then $f = g(x^p) = g_1(x^p)g_2(x^p)$ with each $\deg(g_i(x^p)) \geqslant p \geqslant 1$; this contradicts the fact that f is irreducible.

(iv) $\implies$ (v). By construction, we have $g(x^p) = f$, and so $g(u^p) = f(u) = 0$. It follows that $x - u^p \big| g$ in $\overline{K}[x]$, so there exists $h \in \overline{K}[x]$ such that $g = (x - u^p)h$. Then we have

$$f = g(x^p) = (x^p - u^p)h(x^p) = (x-u)^p h(x^p)$$

where the last step is from the Freshman Dream. It follows that $(x-u)^p \big| f$ in $\overline{K}[x]$.

(v) $\implies$ (vi) $\implies$ (ii). Straightforward. $\square$

15. Day 15

DEFINITION 15.1. Let K be a field, and let $\psi\colon K \to \overline{K}$ be an algebraic closure. Identify K with its image in $\overline{K}$. Let $u \in \overline{K}$, and let $f \in K[x]$ be the minimal polynomial of u.

The element u is *separable* over K if f has no repeated roots in $\overline{K}$. The element u is *inseparable* over K if $u \notin K$ and f has a repeated root in $\overline{K}$.

An irreducible polynomial g is *separable* over K if it has no repeated roots in $\overline{K}$. In general, a polynomial h is *separable* over K if its irreducible factors are all separable. An algebraic extension $\phi\colon K \to L$ is *separable* if every element $v \in L$ is separable over K.

REMARK 15.2. Let K be a field, and let $\psi\colon K \to \overline{K}$ be an algebraic closure. Identify K with its image in $\overline{K}$. Let $u \in \overline{K} - K$, and let $f \in K[x]$ be the minimal polynomial of u.

The element u is inseparable over K if and only if it satisfies the equivalent conditions of Theorem 14.6. Thus, if u is inseparable over K, then *every* root of f is a repeated root with multiplicity at least $p = \mathrm{char}(K)$.

If $u \in K$, then u is separable over K.

Let $g \in K[x]$ be irreducible. Then g is separable over K if and only if $g' \neq 0$. If $g \in K[x]$ is separable (and irreducible), then g has no multiple roots in any extension of K.

If $\mathrm{char}(K) = 0$, then every algebraic extension $K \to L$ is separable. In particular, every algebraic extension $\mathbb{Q} \subseteq L$ is separable.

EXAMPLE 15.3. Consider the extension $k(t^2) \subseteq k(t)$ where t is a variable and $k = \mathbb{Z}/(2)$; see Example 12.3. This extension is not separable because the element $t \in k(t)$ is inseparable over $k(t^2)$. Indeed, we saw that the minimal polynomial of t in $k(t^2)[x]$ is $f = x^2 - t^2$. In $\overline{k(t^2)}[x]$ this factors as $(x-t)^2$, and so t is a multiple root of f in $\overline{k(t^2)}$.

PROPOSITION 15.4. *Let $\phi\colon K \to L$ and $\psi\colon L \to M$ be algebraic field extensions. If M is separable over K, then L is separable over K and M is separable over L.*

PROOF. Let $M \to \overline{M}$ be an algebraic closure, and identify M with its image in $\overline{M}$. Identify L with its image in M, and identify K with its image in L. Thus, we have $K \subseteq L \subseteq M \subseteq \overline{M}$. By assumption, each of these extensions is algebraic, and so $\overline{M}$ is an algebraic closure for K and for L.

Assume that M is separable over K. Then every element of M is separable over K. Thus, every element of $L \subseteq M$ is separable over K, and so L is separable over K.

Let $u \in M$. Let $f \in K[x]$ be the minimal polynomial over K, and let $g \in L[x]$ be the minimal polynomial over L. Since u is separable over K, we know that f has no multiple roots in $\overline{M}$. Since $f \in K[x] \subseteq L[x]$ and $f(u) = 0$, the fact that g is the minial polynomial for u over L implies that $g \big| f$. Since f has no multiple roots in $\overline{M}$, it follows that g has no multiple roots in $\overline{M}$. Thus u is separable over L. Since u is an arbitrary element of M, we conclude that M is separable over L. $\square$

THEOREM 15.5. *Let $\phi\colon K \to L$ be a finite field extension, and let $\psi\colon K \to \overline{K}$ be an algebraic closure. Let $L \to \overline{K}$ be a K-homomorphism and identify L with its image in $\overline{K}$. The following conditions are equivalent:*

(i) *L is separable over K;*
(ii) *$L = K(u_1, \ldots, u_n)$ where each u_i is separable over K;*
(iii) *$|\{K$-homomorphisms $L \to \overline{K}\}| = [L : K]$.*

PROOF. (i) $\implies$ (ii). Since the extension $K \to L$ is finite, we have $L = K(u_1, \ldots, u_n)$ for some $u_i \in L$. Since the extension is separable, each u_i is separable over K.

(ii) $\implies$ (iii). We proceed by induction on n. The base case $n = 1$ follows from Theorem 14.6.

For the induction step, assume that $n > 1$ and that the implication holds for extensions generated by $n - 1$ elements. Note that the proof of Proposition 15.4 shows that u_n is separable over $K(u_1, \ldots, u_{n-1})$. Our induction hypothesis implies that

$$|\{K\text{-homomorphisms } K(u_1, \ldots, u_{n-1}) \to \overline{K}\}| = [K(u_1, \ldots, u_{n-1}) : K].$$

Given a K-homomorphism $K(u_1, \ldots, u_{n-1}) \to \overline{K}$ our base case implies that

$$|\{K(u_1, \ldots, u_{n-1})\text{-homomorphisms } L \to \overline{K}\}| = [L : K(u_1, \ldots, u_{n-1})].$$

This uses the fact that $L = K(u_1, \ldots, u_{n-1})(u_n)$. Lemma 11.8 provides the first equality in the following sequence

$$\begin{aligned} &|\{K\text{-homs } L \to \overline{K}\}| \\ &\qquad = |\{K\text{-homs } K(u_1, \ldots, u_{n-1}) \to \overline{K}\}||\{K(u_1, \ldots, u_{n-1})\text{-homs } L \to \overline{K}\}| \\ &\qquad = [K(u_1, \ldots, u_{n-1}) : K][L : K(u_1, \ldots, u_{n-1})] \\ &\qquad = [L : K]. \end{aligned}$$

The second equality is from the previous two displays, and the third equality is from the Tower Law.

(iii) $\implies$ (i). Let $u \in L$ and suppose that u is not separable over K. Then Theorem 14.6 implies

$$|\{K\text{-homomorphisms } K(u) \to \overline{K}\}| < [K(u) : K].$$

We also have

$$|\{K(u)\text{-homomorphisms } L \to \overline{K}\}| \leqslant [L : K(u)]$$

and so we have

$$\begin{aligned} |\{K\text{-homs } L \to \overline{K}\}| &= |\{K\text{-homs } K(u) \to \overline{K}\}||\{K(u)\text{-homs } L \to \overline{K}\}| \\ &< [K(u) : K][L : K(u)] \\ &= [L : K]. \end{aligned}$$

This is a contradiction. □

16. Day 16

THEOREM 16.1. *Let $\phi\colon K \to L$ and $\psi\colon L \to M$ be finite field extensions. Then M is separable over K if and only if L is separable over K and M is separable over L.*

PROOF. The forward implication is Proposition 15.4. For the reverse implication, assume that L is separable over K and M is separable over L. Thorem 15.5 implies that

$$|\{K\text{-homs } L \to \overline{K}\}| = [L : K]$$

and

$$|\{L\text{-homs } M \to \overline{K}\}| = [M : L].$$

Thus, Lemma 11.8 provides the first equality in the following sequence

$$\begin{aligned} |\{K\text{-homs } M \to \overline{K}\}| &= |\{K\text{-homs } L \to \overline{K}\}||\{L\text{-homs } M \to \overline{K}\}| \\ &= [L : K][M : L] \\ &= [M : K]. \end{aligned}$$

The second equality is from the previous two displays, and the third equality is from the Tower Law. Thus, Thorem 15.5 implies that M is separable over K. □

We are now going to show that every finite separable extension is simple. First some preliminaries.

LEMMA 16.2. *Let $K \to L$ be a finite field extension. If K is finite, then $L = K(u)$ for some $u \in K$.*

PROOF. Since K is finite and $[L : K] < \infty$, we know that L is finite. Hence, Proposition 11.6 implies that the multiplicative group $L^\times$ is cyclic. That is, there is an element $u \in L$ such that $L = \{u^m \mid m \in \mathbb{N}\} \cup \{0\}$. It follows that $L = K(u)$. □

Note that the following result can be used for a previous homework exercise where we find all intermediate fields of $\mathbb{Q} \subseteq \mathbb{Q}(u)$.

LEMMA 16.3. *Let $K \subseteq L = K(u)$ be a simple finite field extension. Let $f \in K[x]$ be the minimal polynomial of u, and let F be an intermediate field of the extension $K \subseteq L = K(u)$. There exists a monic polynomial $g_F = \sum_{i=0}^{d} a_i x^i \in L[x]$ such that $g_F \big| f$ in $L[x]$ and $F = K(a_0, \ldots, a_d)$.*

PROOF. Let $g_F = \sum_{i=0}^{d} a_i x^i \in F[x]$ be the minimal polynomial of u. Since $f \in K[x] \subseteq F[x]$ and $f(u) = 0$, we conclude that $g_F \big| f$. By definition, each $a_i \in F$, and so $K(a_0, \ldots, a_d) \subseteq F$. Since $L = K(u)$ and $K \subseteq F \subseteq L$, we have $L = F(u)$. Since g_F is the minimal polynomial of u over F, we have

$$[L : F] = [F(u) : F] = \deg(g_F) = d.$$

Similarly, we have $L = K(a_0, \ldots, a_d)(u)$. Since $K(a_0, \ldots, a_d) \subseteq L$ and $g_F \in K(a_0, \ldots, a_d)[x]$ and g_F is irreducible in $F[x] \supseteq K(a_0, \ldots, a_d)[x]$, we conclude that g_F is irreducible in $K(a_0, \ldots, a_d)[x]$. Since $g_F(u) = 0$ and g_F is monic, we conclude that g_F is the minimal polynomial of u over $K(a_0, \ldots, a_d)$. Thus, as above we have

$$[L : K(a_0, \ldots, a_d)] = d.$$

the Tower Law implies that

$$d = [L : K(a_0, \ldots, a_d)] = [L : F][F : K(a_0, \ldots, a_d)] = d[F : K(a_0, \ldots, a_d)].$$

We conclude that $[F : K(a_0, \ldots, a_d)] = 1$ and so $F = K(a_0, \ldots, a_d)$. □

THEOREM 16.4 (Primitive Element Theorem). *Let $K \to L$ be a finite field extension, and identify K with its image in L. The following conditions are equivalent:*

(i) *There are only finitely many intermediate fields for the extension $K \subseteq L$;*
(ii) *$L = K(u)$ for some $u \in L$.*

PROOF. (i) $\implies$ (ii). Assume that there are only finitely many intermediate fields for the extension $K \subseteq L$. Since the extension $K \subseteq L$ is finite, there are algebraic elements $u_1, \ldots, u_n \in L$ such that $L = K(u_1, \ldots, u_n)$. We prove that $L = K(u)$ for some $u \in L$ by induction on n. Since the case where K is finite is covered by Lemma 16.2, we assume that K is infinite.

Base case: $n = 2$. Then $L = K(v, w)$ for some $v, w \in L$. For each $a \in L$, the field $K(v + aw)$ is an intermediate field of the extension $K \subseteq L$. Since there are only finitely many intermediate extensions and K is infinite, there are $a, b \in L$ such that $a \neq b$ and $K(v+aw) = K(v+bw)$. Thus, we have $v+aw, v+bw \in K(v+aw)$, and so

$$(a - b)w = (v + aw) - (v + bw) \in K(v + aw).$$

Since $0 \neq a - b \in K$, this implies

$$w = (a - b)^{-1}(a - b)w \in K(v + aw).$$

Since $a \in K$ and $w, a + aw \in K(v + aw)$, this implies that

$$v = (v + aw) - aw \in K(v + aw).$$

That is, we have $v, w \in K(v + aw)$; since $K \subseteq K(v + aw)$, this implies

$$L = K(v, w) \subseteq K(v + aw) \subseteq L$$

and so the element $u = v + aw$ works.

Induction step. Assume that $n > 2$ and that the implication holds for field extensions generated by $n - 1$ elements. Since there are only finitely many intermediate fields for the extension $K \subseteq L$, it follows that, there are only finitely many intermediate fields for the extension $K \subseteq K(u_1, \ldots, u_{n-1})$. Our induction hypothesis implies that $K(u_1, \ldots, u_{n-1}) = K(v)$ for some $v \in K(u_1, \ldots, u_{n-1})$. It follows that

$$L = K(u_1, \ldots, u_{n-1})(u_n) = K(v)(u_n) = K(v, u_n).$$

Since there are only finitely many intermediate fields for the extension $K \subseteq L = K(v, u_n)$, the base case implies that $L = K(u)$ for some $u \in L$.

(ii) $\implies$ (i). Assume that $L = K(u)$ for some $u \in L$. Let $f \in K[x]$ be the minimal polynomial of u. Let F be an intermediate field of the extension $K \subseteq L = K(u)$.

For each intermediate field F of the extension $K \subseteq L$, Lemma 16.3 provides a monic polynomial $g_F = \sum_{i=0}^{d} a_i x^i \in L[x]$ such that $g_F \big| f$ in $L[x]$ and $F = K(a_0, \ldots, a_d)$. The assignment $F \mapsto g_F$ describes a function

$$\Phi\colon \{\text{intermed fields } F \text{ of the extension } K \subseteq L\} \to \{\text{monic factors of } f \text{ in } L[x]\}.$$

Furthermore, the map Φ is 1-1. To see this, assume that $g_F = g_{F'}$. Write $g_F = \sum_{i=0}^{d} a_i x^i$ and $g_{F'} = \sum_{i=0}^{d'} a'_i x^i$. The equality $g_F = g_{F'}$ implies that $d = d'$ and

$$F = K(a_0, \ldots, a_d) = K(a'_0, \ldots, a'_d) = F'$$

as desired.

Since the number of monic factors of f in $L[x]$ is finite, it follows that the set of intermediate fields of the extension $K \subseteq L$ is also finite. □

17. Day 17

THEOREM 17.1. *Let $K \to L$ be a finite field extension. If L is separable over K, then $L = K(u)$ for some $u \in L$.*

PROOF. The case where K is finite is covered by Lemma 16.2, so we assume that K is infinite. Furthermore, we assume that $L = K(v, w)$ for some $v, w \in L$. (The general case follows by induction as in the proof of the implication (i) $\implies$ (ii) in Theorem 16.4.) Let $K \to \overline{K}$ be an algebraic closure, and let $L \to \overline{K}$ be a K-homomorphism. Identify L with its image in $\overline{K}$, and identify K with its image in L.

Let $\sigma_1, \ldots, \sigma_n$ be the distinct K-homomorphisms $L \to \overline{K}$. (Recall that $n \leqslant [L : K]$ by Theorem 12.1.) Consider the polynomial

$$P = \prod_{i \neq j} [(\sigma_i(v) + \sigma_i(w)x) - (\sigma_j(v) + \sigma_j(w)x)] \in \overline{K}[x].$$

Claim: $P \neq 0$. If $P = 0$, then $\sigma_i(v) + \sigma_i(w)x = \sigma_j(v) + \sigma_j(w)x$ for some $i \neq j$. By equating coefficients, we see that $\sigma_i(v) = \sigma_j(v)$ and $\sigma_i(w) = \sigma_j(w)$. Since $\sigma_i, \sigma_j \colon L = K(v, w) \to \overline{K}$ is a K-homomorphism, this implies that $\sigma_i = \sigma_j$, contradicting the condition $i \neq j$.

Now, the polynomial P has finitely many roots in K. Since K is infinite, this implies that there is an element $a \in K$ such that $P(a) \neq 0$. Thus, for all $i \neq j$, we have

$$\sigma_i(v) + \sigma_i(w)a \neq \sigma_j(v) + \sigma_j(w)a.$$

Since σ_i and σ_j are K-homomorphisms and $a \in K$, this reads as

$$\sigma_i(v) + \sigma_i(wa) \neq \sigma_j(v) + \sigma_j(wa)$$
$$\sigma_i(v + wa) \neq \sigma_j(v + wa)$$

which holds for all $i \neq j$.

Claim: $L = K(v + wa)$. Suppose not. Then we have $K(v + wa) \subsetneq L$, and so $1 < [L : K(v + wa)] < \infty$. Since L is separable over K, Proposition 15.4 implies that L is separable over $K(v + wa)$. Hence, Theorem 15.5 implies that

$$|\{K(v + wa)\text{-homs } L \to \overline{K}\}| = [L : K(v + wa)] > 1.$$

Let $\sigma \colon L \to \overline{K}$ be a non-identity $K(v + wa)$-homomorphism. Then σ is a K-homomorphism $L \to \overline{K}$, and so $\sigma = \sigma_i$ for some i. Also, the identity $\mathrm{id}_L \colon L \to L \subseteq \overline{K}$ is a K-homomorphism, and so $\mathrm{id}_L = \sigma_j$ for some $j \neq i$. Since σ_i is a $K(v + wa)$-homomorphism, we have

$$\sigma_i(v + wa) = v + wa = \sigma_j(v + wa)$$

contradicting the previous paragraph. □

Here is an example of a finite field extension that is not simple.

EXAMPLE 17.2. Let p be a prime integer and set $k = \mathbb{Z}/(p)$. Let $L = k(s, t)$ denote the field of rational functions in two variables s and t, and set $K = k(s^p, t^p) \subseteq K(s, t) = L$. The element $s \in L$ is not in K, and is a root of the polynomial $f = x^p - s^p \in K[x]$. In $L[x]$, this polynomial splits as $f = x^p - s^p = (x - s)^p$.

Claim: $f = x^p - s^p$ is irreducible in $K[x]$. Let $g \in K[x]$ be the minimal polynomial for s. Since $s \notin K$, we know $d = \deg(g) > 1$. Since $f(s) = 0$, we know $g \big| f$ in $K[x]$. This implies that $g \big| f = (x-s)^p$ in $L[x]$, and so $g = (x-s)^d$. This implies that s is a multiple root of g in $\overline{K}$, and so Theorem 14.6 implies that $(x-s)^p \big| g$ in $\overline{K}[x]$. Thus, we have $p \leqslant d \leqslant p$ and so $p = d$, which implies that $g = f$.

It follows that the extension $K \subseteq K(s)$ has degree p. A similar argument shows that the extension $K(s) \subseteq K(s,t) = L$ has degree p. Hence, the Tower Law implies that $[L : K] = p^2$.

Suppose that there exists $u \in L$ such that $K(s,t) = L = K(u)$. Then we can write $u = v(s,t)/w(s,t)$ for some $v, w \in k[x,y]$. It follows from the Freshman Dream that $u^p = v(s^p, t^p)/w(s^p, t^p) \in K$, and so $[K(u) : K] \leqslant p < p^2$. Since $[L : K] = p^2$, we cannot have $L = K(u)$.

LEMMA 17.3. *A finite field extension $K \subseteq L$ is Galois if and only if it is normal and separable.*

PROOF. Combine Proposition 12.6 and Theorems 13.1 and 15.5. □

THEOREM 17.4. *Let $p > 0$ be a prime integer and let $n \geqslant 1$ be an integer. Then there exists a field k such that $|k| = p^n$, and k is unique up to isomorphism. Also, k is a splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{Z}/(p)$, and we have $a^{p^n} = a$ for all $a \in k$. Also, the extension $\mathbb{Z}/(p) \subseteq k$ is Galois.*

PROOF. Case 1: $n = 1$. The field $\mathbb{Z}/(p)$ has order p. Use the characteristic homomorphism to show that, if k is a field of order p, then $k \cong \mathbb{Z}/(p)$. We know that $a^p = a$ for all $a \in k = \mathbb{Z}/(p)$ by Fermat's Little Theorem. It follows that k is a splitting field of the polynomial $X^p - X$ over $\mathbb{Z}/(p)$.

Case 2: $n > 1$. Let k be a the splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{Z}/(p)$. Let $K = \{a \in k \mid a^{p^n} = a\}$. Use the Freshman Dream to show that K is a subfield of k. By definition, we know that every element of K is a root of the polynomial $X^{p^n} - X$. Since k is generated over $\mathbb{Z}/(p)$ by the roots of $X^{p^n} - X$, we conclude that $K = k$. Hence, the extension $\mathbb{Z}/(p) \subseteq k$ is normal.

We have $(X^{p^n} - X)' = -1$, and so $X^{p^n} - X$ has no multiple roots in any extension of $\mathbb{Z}/(p)$. It follows that $X^{p^n} - X$ has exactly p^n roots in k. Since $k = K$, it follows that $|k| = p^n$. It follows that the extension $\mathbb{Z}/(p) \subseteq k$ is separable and hence Galois.

Let L be a field with $|L| = p^n$. We know that the multiplicative group $L^\times$ is cyclic of order $p^n - 1$. It follows that $b^{p^n - 1} = 1$ for all $b \in L^\times$, and so $c^{p^n} = c$ for all $c \in L$. Since L has exactly p^n elements, that is, the number of roots of $X^{p^n} - X$, it follows that L is a splitting field of $X^{p^n} - X$ over $\mathbb{Z}/(p)$. Since splitting fields are unique up to isomorphism, we have $L \cong K$. □

18. Day 18

Now we go for the Galois correspondence.

LEMMA 18.1. *Let $K \subseteq L$ be a finite separable field extension, and let $n \geqslant 1$. Assume that, for every element $a \in L$, there is a polynomial $f \in K[x]$ such that $f(a) = 0$ and $\deg(f) \leqslant n$. Then $[L : K] \leqslant n$.*

PROOF. The separability assumption implies that $L = K(u)$ for some $u \in L$. The polynomial hypothesis implies that the minimal polynomial of u over K has degree $\leqslant n$, and so $[L : K] \leqslant n$. □

DEFINITION 18.2. Let L be a field, and let H be a finite group of automorphisms $L \to L$. The *fixed field* of H is

$$L^H = \{a \in L \mid f(a) = a \text{ for all } f \in H\}.$$

It is straightforward to show that L^H is a subfield of L. If H is a group of K-automorphisms, where K is a subfield of L, then L^H is an intermediate field of the extension $K \subseteq L$.

REMARK 18.3. Let $K \subseteq L$ be a finite field extension, and recall that the Galois group of this extension is the group

$$\mathrm{Gal}(L : K) = \{K\text{-homomorphisms } L \to L\}.$$

This is a group under composition since each K-homomorphism $L \to L$ is an isomorphism. It is also finite because $|\operatorname{Gal}(L : K) \leqslant [L : K] < \infty$.

Let F be an intermediate field of the extension $K \subseteq L$. Then we have

$$\mathrm{Gal}(L : F) \leqslant \mathrm{Gal}(L : K)$$

because every F-homomorphism $L \to L$ is also a K-homomorphism, and because the operation on each group is composition.

The Galois correspondence says that, if the extension $K \subseteq L$ is Galois, then there is a 1-1 correspondence

$$\{\text{intermediate fields } K \subseteq F \subseteq L\} \longleftrightarrow \{\text{subgroups } H \leqslant \mathrm{Gal}(L : K)\}$$

given by

$$F \longmapsto \mathrm{Gal}(L : F)$$
$$L^H \longmapsfrom H.$$

It also says more, but we'll get to that later.

LEMMA 18.4. *Let $K \subseteq L$ be a finite field extension, and let $H \leqslant \mathrm{Gal}(L : K)$ with fixed field L^H. Then $|H| = [L : L^H]$, the extension $L^H \subseteq L$ is Galois, and $\mathrm{Gal}(L : L^H) = H$.*

PROOF. We have subfields $K \subseteq L^H \subseteq L$. Since $K \subseteq L$ is finite, it follows that $L^H \subseteq L$ is finite. By definition, we have $H \subseteq \mathrm{Gal}(L : L^H)$, and so $|H| \leqslant |\operatorname{Gal}(L : L^H)|$.

Let $a \in L$, and let $f_1(a), \dots, f_k(a) \in L$ be the distinct images of a under H. Assume without loss of generality that $f_1 = \mathrm{id}_L$, and so $f_1(a) = a$. For each $g \in H$, the list $g(f_1(a)), \dots, g(f_k(a)) \in L$ is a list of distinct images of a under H. (They are images under H because $g, f_i \in H$ implies that $gf_i \in H$. They are distinct because f is 1-1.) It follows that the list $g(f_1(a)), \dots, g(f_k(a))$ is a permutation of the list $f_1(a), \dots, f_k(a)$.

Set $h = (x - f_1(a)) \cdots (x - f_k(a)) \in L[x]$ which has degree $k \leqslant |H|$. The automorphism g permutes the roots of h, and so g fixes the coefficients of h. That is, the coefficients of h are in L^H. Since $f_1(a) = a$, it follows that a is a root of h. Since the roots of h are distinct, it follows that the roots of the minimal polynomial of a over L^H are distinct, and so the extension $L^H \subseteq L$ is separable. Since this

extension is finite and every element of L satisfies a polynomial with coefficients in L^H of degree $\leqslant |H|$, Lemma 18.1 implies $[L : L^H] \leqslant |H|$. With the first paragraph and Corollary 12.2, this implies

$$|H| \leqslant |\operatorname{Gal}(L : L^H)| \leqslant |\{L^H\text{-homs } L \to \overline{L^H}\}| \leqslant [L : L^H] \leqslant |H|.$$

It follows that we have equality at each step of the display. Equality at the first step implies that $\operatorname{Gal}(L : L^H) = H$. Equality at the second and third steps imply that the extension $L^H \subseteq L$ is Galois. Equality at the fourth step implies that $|H| = [L : L^H]$. □

THEOREM 18.5 (Galois Correspondence, part 1). *Let $K \subseteq L$ be a finite Galois extension. There is a 1-1 containment-reversing correspondence*

$$\{\textit{intermediate fields } K \subseteq F \subseteq L\} \longleftrightarrow \{\textit{subgroups } H \leqslant \operatorname{Gal}(L : K)\}$$

given by

$$F \longmapsto \operatorname{Gal}(L : F)$$
$$L^H \longmapsfrom H.$$

If F is an intermediate field of the extension $K \subseteq L$, then the extension $F \subseteq L$ is Galois and the extension $K \subseteq F$ is separable.

PROOF. Let

$$S = \{\text{subgroups } H \leqslant \operatorname{Gal}(L : K)\}$$
$$I = \{\text{intermediate fields } K \subseteq F \subseteq L\}.$$

0. For each $F \in I$, the extension $K \subseteq F$ is separable by Theorem 16.1. Also, the extension $F \subseteq L$ is Galois, as follows. The extension $K \subseteq L$ is separable, and so the extension $F \subseteq L$ is separable by Theorem 16.1. The extension $K \subseteq L$ is normal, and so L is a splitting field over K for some polynomial $f \in K[x]$. It follows that L is a splitting field over F for the same polynomial $f \in K[x] \subseteq F[x]$, and so the extension $F \subseteq L$ is normal.

1. Check that, if $H, H' \in S$ and $H \subseteq H'$, then $L^{H'} \subseteq L^H$.

2. Check that, if $F, F' \in I$ and $F \subseteq F'$, then $\operatorname{Gal}(L : F') \subseteq \operatorname{Gal}(L : F)$.

3. Let $\mathcal{G}\colon I \to S$ be given by $\mathcal{G}(F) = \operatorname{Gal}(L : F)$. Let $\mathcal{F}\colon S \to I$ be given by $\mathcal{F}(H) = L^H$. We need to show that $\mathcal{F}(\mathcal{G}(F)) = F$ for all $F \in I$ and $\mathcal{G}(\mathcal{F}(H)) = H$ for all $H \in S$.

4. Lemma 18.4 implies that, for each $H \in S$, we have $H = \operatorname{Gal}(L : L^H) = \mathcal{G}(L^H) = \mathcal{G}(\mathcal{F}(H))$.

5. Part 1 translates as: If $H, H' \in S$ and $H \subseteq H'$, then $\mathcal{F}(H') \subseteq \mathcal{F}(H)$.

6. Part 2 translates as: If $F, F' \in I$ and $F \subseteq F'$, then $\mathcal{G}(F') \subseteq \mathcal{G}(F)$.

7. If $F \in I$, then $\mathcal{F}(\mathcal{G}(F)) \supseteq F$. Indeed, each $g \in \operatorname{Gal}(L : F) = \mathcal{G}(F)$ fixes F and so $F \subseteq L^{\mathcal{G}(F)} = \mathcal{F}(\mathcal{G}(F))$.

8. For each $F \in I$, we have $\mathcal{G}(\mathcal{F}(\mathcal{G}(F))) = \mathcal{G}(F)$: use $H = \mathcal{G}(F)$ in part 4.

9. For each $H \in S$ and each $F \in I$, we have $H \subseteq \mathcal{G}(F)$ if and only if $F \subseteq \mathcal{F}(H)$. Indeed, if $H \subseteq \mathcal{G}(F)$, then H fixes every element of F, and so $F \subseteq \mathcal{F}(H)$. On the other hand, if $F \subseteq \mathcal{F}(H)$, then F is fixed by every element of H, and so $H \subseteq \mathcal{G}(F)$.

10. $\mathcal{F}(\mathcal{G}(F)) = F$ for all $F \in I$. The extension $F \subseteq L$ is Galois by part 0. Hence, we have

$$|\mathcal{G}(F)| = |\operatorname{Gal}(L : F)| = [L : F].$$

Part 8 implies $\mathcal{G}(\mathcal{F}(\mathcal{G}(F))) = \mathcal{G}(F)$. Part 7 says $F \subseteq \mathcal{F}(\mathcal{G}(F)) \subseteq L$, and so

$$[L : \mathcal{F}(\mathcal{G}(F))] \geqslant |\mathcal{G}(\mathcal{F}(\mathcal{G}(F)))| = |\mathcal{G}(F)| = [L : F] \geqslant [L : \mathcal{F}(\mathcal{G}(F))].$$

It follows that we have equality at each step. Equality at the last step, with the Tower Law, implies $\mathcal{F}(\mathcal{G}(F)) = F$. □

19. Day 19

LEMMA 19.1. *Let $K \subseteq L$ be a finite Galois extension, and let F be an intermediate field of the extension $K \subseteq L$. Let $H = \mathrm{Gal}(L : F) \leqslant \mathrm{Gal}(L : K)$ be the subgroup corresponding to F under the Galois correspondence, and let $g \in \mathrm{Gal}(L : K)$. Then the subgroup of $\mathrm{Gal}(L : K)$ corresponding to $g(F) \subseteq L$ under the Galois correspondence is exactly gHg^{-1}.*

PROOF. By construction, we need to show that

$$\mathrm{Gal}(L : g(F)) = g\,\mathrm{Gal}(L : F)g^{-1}.$$

$\supseteq$: Let $h \in \mathrm{Gal}(L : F)$. We need to show that $ghg^{-1} \in \mathrm{Gal}(L : g(F))$, that is, we need to show that ghg^{-1} is a K-homomorphism $L \to L$ that fixes $g(F)$. Since $g, h \in \mathrm{Gal}(L : K)$ and $\mathrm{Gal}(L : K)$ is a group, we know that ghg^{-1} is a K-homomorphism $L \to L$. To see that ghg^{-1} fixes $g(L)$, let $g(y) \in g(L)$. Then we have

$$ghg^{-1}(g(y)) = gh(y) = g(y)$$

where the first equality is by definition. The second equality is from the fact that $h \in \mathrm{Gal}(L : F)$, which means that h fixes every element of F.

$\subseteq$: From the previous paragraph, we have

$$\begin{aligned}\mathrm{Gal}(L : g(F)) &= g(g^{-1}\,\mathrm{Gal}(L : g(F))g)g^{-1} \\ &\subseteq g\,\mathrm{Gal}(L : g^{-1}(g(F)))g^{-1} = g\,\mathrm{Gal}(L : F)g^{-1}\end{aligned}$$

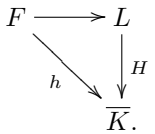
□

LEMMA 19.2. *Let $K \subseteq L$ be a finite Galois extension, and let F be an intermediate field of the extension $K \subseteq L$. The extension $K \subseteq F$ is normal if and only if, for each $g \in \mathrm{Gal}(L : K)$, we have $g(F) = F$ (equivalently, $g(F) \subseteq F$).*

PROOF. Assume that $K \subseteq F \subseteq L \subseteq \overline{K}$ where $\overline{K}$ is an algebraic closure for K.

$\Longrightarrow$: Assume that $K \subseteq F$ is normal, and let $g \in \mathrm{Gal}(L : K)$. Then g is a K-homomorphism $L \to L \subseteq \overline{K}$. Thus, g restricts to a K-homomorphism $F \to \overline{K}$. Since $K \subseteq F$ is normal, we have $g(F) = F$ by Theorem 13.1.

$\Longleftarrow$: Assume that, for each $g \in \mathrm{Gal}(L : K)$, we have $g(F) \subseteq F$. Let $h\colon F \to \overline{K}$ be a K-homomorphism. By Theorem 13.1 we need to show that $h(F) \subseteq F$. Theorem 10.2 implies that there is a field homomorphism $H\colon L \to \overline{K}$ making the following diagram commute:



Here, the unlabeled map is the inclusion. Since h is a K-homomorphism, it follows that H is a K-homomorphism. The extension $K \subseteq L$ is Galois, hence normal, and

so $H(L) = L$. In other words, we have $H \in \operatorname{Gal}(L : K)$, so our assumption implies that $h(F) = H(F) \subseteq F$ as desired. □

LEMMA 19.3. *Let $K \subseteq L$ be a finite Galois extension, and let F be an intermediate field of the extension $K \subseteq L$. The extension $K \subseteq F$ is normal if and only if, for each $g \in \operatorname{Gal}(L : K)$, we have $g \operatorname{Gal}(L : F)g^{-1} = \operatorname{Gal}(L : F)$ (equivalently, $g \operatorname{Gal}(L : F)g^{-1} \subseteq \operatorname{Gal}(L : F)$).*

PROOF. $\Longrightarrow$: Assume that $K \subseteq F$ is normal, and let $g \in \operatorname{Gal}(L : K)$. By Lemma 19.2 we have $g(F) = F$. Lemma 19.1 implies that

$$g \operatorname{Gal}(L : F)g^{-1} = \operatorname{Gal}(L : g(F)) = \operatorname{Gal}(L : F).$$

$\Longleftarrow$: Assume that $g \operatorname{Gal}(L : F)g^{-1} \subseteq \operatorname{Gal}(L : F)$ for each $g \in \operatorname{Gal}(L : K)$; it follows from standard group theory that we have $g \operatorname{Gal}(L : F)g^{-1} = \operatorname{Gal}(L : F)$. By Lemma 19.2 we need to show that, for each $g \in \operatorname{Gal}(L : K)$, we have $g(F) \subseteq F$. Let $g \in \operatorname{Gal}(L : K)$. Lemma 19.1 implies

$$\operatorname{Gal}(L : g(F)) = g \operatorname{Gal}(L : F)g^{-1} = \operatorname{Gal}(L : F).$$

Theorem 18.5 implies that

$$g(F) = L^{\operatorname{Gal}(L:g(F))} = L^{\operatorname{Gal}(L:F)} = F$$

as desired. □

THEOREM 19.4 (Galois Correspondence, part 2). *Let $K \subseteq L$ be a finite Galois extension, and let F be an intermediate field of the extension $K \subseteq L$.*

(a) *The extension $K \subseteq F$ is normal (i.e., Galois) if and only if* $\operatorname{Gal}(L : F) \trianglelefteq \operatorname{Gal}(L : K)$.
(b) *We have* $[F : K] = [\operatorname{Gal}(L : K) : \operatorname{Gal}(L : F)]$.
(c) *If $K \subseteq F$ is normal, then* $\operatorname{Gal}(F : K) \cong \operatorname{Gal}(L : K)/\operatorname{Gal}(L : F)$.

PROOF. (a) This is precisely Lemma 19.3.

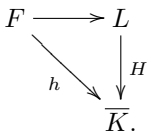
(b) Since $K \subseteq L$ is Galois, we have $[L : K] = |\operatorname{Gal}(L : K)|$. Lemma 18.4 implies

$$\begin{aligned} [L : K] &= |\operatorname{Gal}(L : K)| \\ [L : F][F : K] &= |\operatorname{Gal}(L : F)|[\operatorname{Gal}(L : K) : \operatorname{Gal}(L : F)] \\ |\operatorname{Gal}(L : F)|[F : K] &= |\operatorname{Gal}(L : F)|[\operatorname{Gal}(L : K) : \operatorname{Gal}(L : F)] \\ [F : K] &= [\operatorname{Gal}(L : K) : \operatorname{Gal}(L : F)] \end{aligned}$$

(c) Assume that $K \subseteq F$ is normal. Lemma 19.2 implies that $g(F) = F$ for each $g \in \operatorname{Gal}(L : K)$. In other words, for each $g \in \operatorname{Gal}(L : K)$, the restriction $g|_F$ is a K-homomorphism $F \to F$.

Define $\Phi\colon \operatorname{Gal}(L : K) \to \operatorname{Gal}(F : K)$ by restriction: $\Phi(g) = g|_F$. The previous paragraph implies that this is well-defined. It is straightfoward to show that Φ is a group homomorphism.

Claim: Φ is onto. Let $h \in \operatorname{Gal}(F : K)$. Theorem 10.2 implies that there is a field homomorphism $H\colon L \to \overline{K}$ making the following diagram commute:



Here, the unlabeled map is the inclusion. Since h is a K-homomorphism, it follows that H is a K-homomorphism. The extension $K \subseteq L$ is Galois, hence normal, and so $H(L) = L$. In other words, we have $H \in \mathrm{Gal}(L : K)$. The commutativity of the diagram implies that $h = H|_F = \Phi(H)$, establishing the claim.

Claim: $\mathrm{Ker}(\Phi) = \mathrm{Gal}(L : F)$. (Once we show this, then the isomorphism follows from your favorite isomorphism theorem: $\mathrm{Gal}(F : K) \cong \mathrm{Gal}(L : K)/\mathrm{Ker}(\Phi)$.) A K-homomorphism $g \in \mathrm{Gal}(L : K)$ is in $\mathrm{Ker}(\Phi)$ if and only if $g|_F = \mathrm{id}_F$, that is, if and only if g is an F-homomorphism $L \to L$, that is, if and only if $g \in \mathrm{Gal}(L : F)$. □

20. Day 20

Now we compute some Galois groups and some intermediate fields. Part (d) of the next result shows how knowledge of the Galois group gives you information about the structure of the intermediate fields of an extension.

Proposition 20.1. *Let $K \subseteq L$ be an extension of finite fields.*

(a) *Then $|K| = p^n = q$ where $p = \mathrm{char}(K) \geqslant 1$ and $n \geqslant 1$. Also, $|L| = q^d$ where $d = [L : K] \geqslant 1$.*
(b) *The extension $K \subseteq L$ is Galois with cyclic Galois group $\mathrm{Gal}(L : K) = \langle g \rangle \cong \mathbb{Z}/(d)$ where $g\colon L \to L$ is given by $a \mapsto a^q$.*
(c) *The intermediate fields of this extension are exactly the fields of the form $F_k = \{a \in L \mid a^{q^k} = a\}$ with $k = 1, \ldots, d$. (Note that these fields are not necessarily distinct.)*
(d) *Under the Galois correspondence, the field F_k corresponds to the cyclic subgroup $\langle g^k \rangle \leqslant \mathrm{Gal}(L : K)$.*

Proof. (a). Since K is finite, it cannot contain a copy of $\mathbb{Q}$. It follows from an exercise that $\mathrm{char}(K) \neq 0$ and so $\mathrm{char}(K) = p \geqslant 1$. Since K is then a finite extension of $\mathbb{Z}/(p)$, we have $|K| = p^n = q$ where $n = [K : \mathbb{Z}/(p)]$. Since L is finite and an extension of K, it is a finite extension of K, so we have $|L| = q^d$ where $d = [L : K] \geqslant 1$.

(b). From Theorem 17.4 we know that the extension $\mathbb{Z} \subseteq K$ is Galois, as is the extension $\mathbb{Z}/(p) \subseteq L$. Since K is an intermediate field of the Galois extension $\mathbb{Z}/(p) \subseteq L$, Theorem 18.5 implies that the extension $K \subseteq L$ is Galois.

Let $g\colon L \to L$ be given by $a \mapsto a^q$. The Freshman Dream implies that g is a field homomorphism. From Theorem 17.4 we know that $a^q = a$ for all $a \in K$. In other words, we have $g(a) = a$ for all $a \in K$, and so $g \in \mathrm{Gal}(L : K)$. Note that, for each $r \in \mathbb{N}$ we have $g^r(a) = a^{q^r}$ for all $a \in L$. It follows that $|g| \leqslant d$ in $\mathrm{Gal}(L : K)$ because $g^d(a) = a^{q^d} = a$ for all $a \in L$; the last equality follows from Theorem 17.4 because $|L| = q^d$.

Claim: $|g| = d$ in $\mathrm{Gal}(L : K)$. Suppose that $0 < r \leqslant d$ and $g^r = \mathrm{id}_L$. Then $a = g^r(a) = a^{a^r}$ for all $a \in L$. In other words, every element of L is a root of the nonconstant polynomial $x^{q^r} - x$. this polynomial has at most q^r roots, and so $q^d = |L| \leqslant q^r$. It follows that $d \leqslant r$, and since $r \leqslant d$ by assumption, we have $r = d$. This completes the proof of the claim.

The extension $K \subseteq L$ is Galois, and so

$$|\,\mathrm{Gal}(L : K)| = [L : K] = d.$$

We have just shown that $g \in \mathrm{Gal}(L:K)$ is an element of order d. It follows that $\mathrm{Gal}(L:K)$ is cyclic generated by g.

(c) and (d). The subgroups of $\mathrm{Gal}(L:K) = \langle g \rangle$ are all of the form $\langle g^k \rangle$ for $k = 1, \ldots, d$. It is straightforward to show that F_k is the fixed field of $\langle g^k \rangle$. The fact that these are the only intermediate fields follows from the Galois correspondence. □

Recall that every finite group G is isomorphic to a subgroup of S_n where $n = |G|$. Here is a similar result for Galois groups. Note that the conclusion of part (b) holds without the separable hypothesis.

PROPOSITION 20.2. *Let K be a field and let $f \in K[x]$ be a polynomial of degree $n \geqslant 1$. Let L be a splitting field of f over K.*

(a) *The action of* $\mathrm{Gal}(L:K)$ *on the set of roots of f yields a monomorphism of groups* $\mathrm{Gal}(L:K) \hookrightarrow S_n$.
(b) *If the extension $K \subseteq L$ is separable (e.g., if* $\mathrm{char}(K) = 0$*), then* $[L:K] \big| n!$.

PROOF. (a) Let $a_1, \ldots, a_d \in L$ be the distinct roots of f in L. Since $d \leqslant n$, there is a monomorphism of groups $S_d \hookrightarrow S_n$. Hence, it suffices to construct a monomorphism of groups $\phi\colon \mathrm{Gal}(L:K) \hookrightarrow S_d$.

Let $g \in \mathrm{Gal}(L:K)$. For each i, the element $g(a_i)$ is a root of f. Furthermore, if $i \neq j$, then $g(a_i) \neq g(a_j)$ since g is 1-1. Hence, g permutes the roots of f. That is, there is an element $\sigma_g \in S_d$ such that $g(a_i) = a_{\sigma_g(i)}$ for each i.

For each $g, h \in \mathrm{Gal}(L:K)$ and each i, we have

$$a_{\sigma_{hg}(i)} = h(g(a_i)) = h(a_{\sigma_g(i)}) = a_{\sigma_h(\sigma_g(i))}.$$

Since the a_j are distinct, this implies that $\sigma_{hg} = \sigma_h \sigma_g$. Hence the assignment $g \mapsto \sigma_g$ describes a group homomorphism $\phi\colon \mathrm{Gal}(L:K) \to S_d$. It remains to show that ϕ is 1-1.

Let $g \in \mathrm{Ker}(\phi)$. Then $g(a_i) = a_i$ for $i = 1, \ldots, d$. Since L is a splitting field for K, we have $L = K(a_1, \ldots, a_d)$, and so the K-homomorphism $g\colon L \to L$ is completely determined by its action on the a_i. It follows that $g = \mathrm{id}_L$, and so ϕ is 1-1.

(b) Assume that the extension $K \subseteq L$ is separable, i.e. Galois. Then we have

$$[L:K] = |\mathrm{Gal}(L:K)| \big| |S_n| = n!$$

as desired. □

The next example shows that the map $\mathrm{Gal}(L:K) \hookrightarrow S_n$ need not be surjective, even when f is irreducible and the extension $K \subseteq L$ is Galois.

EXAMPLE 20.3. Let $L \subseteq \mathbb{C}$ be a splitting field over $K = \mathbb{Q}$ of the cyclotomic polynomial $f = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$. Recall that f is irreducible by Eisenstein's criterion. The extension $K \subseteq L$ is normal because L is a splitting field over K, and it is separable because $\mathrm{char}(K) = 0$. Let $w = e^{2\pi i/5} \in \mathbb{C}$. Then the distinct roots of f in L are w, w^2, w^3, w^4 so we have $L = K(w, w^2, w^3, w^4) = K(w)$. It follows that $[L:K] = \deg(f) = 4$.

Proposition 20.2 gives a group monomorphism $\phi\colon \mathrm{Gal}(L:K) \hookrightarrow S_4$. The extension $K \subseteq L$ is Galois, so we have

$$|\mathrm{Gal}(L:K)| = [L:K] = 4 < 4! = |S_4|.$$

Hence the map ϕ cannot be onto. In fact, since $|\mathrm{Gal}(L:K)| = 4$, we know that $\mathrm{Gal}(L:K) \ncong S_n$ for all n.

THEOREM 20.4. *Let G be a finite group. There exists a finite Galois extension $K \subseteq L$ such that* $\mathrm{Gal}(L : K) \cong G$.

PROOF. Case 1: $G = S_n$. Let $L = \mathbb{Q}(x_1, \ldots, x_n)$, the field of rational functions in n variables over $\mathbb{Q}$. Each $g \in S_n$ induces a $\mathbb{Q}$-isomorphism $\phi_g \colon L \to L$ by permuting the variables. Furthermore, the set $H = \{\phi_g \mid g \in S_n\}$ is a group of isomorphisms $L \to L$ and that the assignment $g \mapsto \phi_g$ describes a group isomorphism $S_n \to H$. Let $K = L^{S_n}$ be the fixed field.

Let $f = (x - x_1)(x - x_2) \cdots (x - x_n) \in L[x]$. Since the elements of H only permute the roots of f, we see that the coefficients of f are fixed by H. In other words, we have $f \in K[x]$. Since each generator $x_i \in L$ is a root of f, we see that the extension $K \subseteq L$ is finite. By construction, we have $H \leqslant \mathrm{Gal}(L : K)$, and so Lemma 18.4 implies that the extension $K \subseteq L$ is Galois with Galois group $\mathrm{Gal}(L : K) = G \cong S_n$.

Case 2: The general case. Identify G with a subgroup of S_n for some n. By case 1, there is a finite Galois extension $K \subseteq L$ such that $\mathrm{Gal}(L : K) \cong S_n$. Lemma 18.4 implies that the extension $L^G \subseteq L$ is Galois with Galois group $\mathrm{Gal}(L : L^G) \cong G$. □

Here is a very big open question in the area. The answer is known when G is solvable, but not in general.

QUESTION 20.5. Let G be a finite group. Does there exists a finite Galois extension $\mathbb{Q} \subseteq L$ such that $\mathrm{Gal}(L : \mathbb{Q}) \cong G$?

21. Day 21

THEOREM 21.1 (Fundamental Thm. of Algebra). *The field $\mathbb{C}$ is algebraically closed.*

PROOF. Claim 1: There are no finite extensions $\mathbb{R} \subseteq L$ of odd degree. The primitive element theorem implies that $L = \mathbb{R}(a)$ for some $a \in L$. If $[L : \mathbb{R}]$ is odd, then so is the degree of the minimal polynomial f of a over $\mathbb{R}$ (since these numbers are equal). The Intermediate Value Theorem from calculus implies that f has a real root, so it is not irreducible, a contradiction.

Claim 2: There is no extension $\mathbb{C} \subseteq E$ of degree 2. Suppose that $[E : \mathbb{C}] = 2$. It follows that $E = \mathbb{C}[u]$ for some $u \in E$, in fact, for each $u \in E - \mathbb{C}$. Since $[E : \mathbb{C}] = 2$, the minimal polynomial of u in $\mathbb{C}[x]$ has degree 2. Write it as $f = x^2 + bx + c$. It is straightforward to show that $\mathbb{C}$ contains a square root of $b^2 - 4c$. Let $w \in \mathbb{C}$ be such a quare root. It is straightforward to show that the elements $\frac{-b \pm w}{2} \in \mathbb{C}$ is a root of f, contradicting the fact that f is irreducible.

Let $\mathbb{C} \subseteq F$ be a finite field extension. It suffices to show that $\mathbb{C} = F$.

Case 1: The extension $\mathbb{R} \subseteq F$ is Galois. Let $G = \mathrm{Gal}(L : \mathbb{R})$. Theorem 18.5 implies that the extension $\mathbb{C} \subseteq F$ is Galois.

Claim 3: $|G| = 2^k$ for some k. Suppose not. Let $H \leqslant G$ be a 2-Sylow subgroup, and let $F^H \subseteq F$ be the fixed field of H. Theorem 19.4(b) implies that $[F^H : \mathbb{R}] = [G : H]$ which is odd. This contradicts the first claim.

Suppose that $\mathbb{C} \neq F$. The previous claim implies that $[F : \mathbb{R}] = 2^k$ and so $|\mathrm{Gal}(F : \mathbb{C})| = [F : \mathbb{C}] = 2^{k-1} > 1$. Fix a subgroup $K \leqslant \mathrm{Gal}(F : \mathbb{C})$ such that $[\mathrm{Gal}(F : \mathbb{C}) : K] = 2$. (Use the fact that the center $Z(\mathrm{Gal}(F : \mathbb{C}))$ is nontrivial and argue by induction on k.) Since $[\mathrm{Gal}(F : \mathbb{C}) : K] = 2$, we know that $K \trianglelefteq \mathrm{Gal}(F :$

$\mathbb{C}$). We now employ Theorem 19.4. The corresponding fixed field F^K is a Galois extension of $\mathbb{C}$ because $K \trianglelefteq \operatorname{Gal}(F : \mathbb{C})$. Hence, it satisfies

$$[F^K : \mathbb{C}] = |\operatorname{Gal}(F^K : \mathbb{C})| = |\operatorname{Gal}(F : \mathbb{C})/K| = [\operatorname{Gal}(F : \mathbb{C}) : K] = 2.$$

This contradicts Claim 2.

Case 2: The general case. Let $F = \mathbb{R}(a_1, \ldots, a_n)$, and let $f_i \in \mathbb{R}[x]$ be the minimal polynomial of a_i. Let $f = f_1 \cdots f_n$ and let F' be a splitting field of f over F. Then F' is a splitting field of f over $\mathbb{R}$, so the extension $\mathbb{R} \subseteq F'$ is normal. It is separable because $\operatorname{char}(\mathbb{R}) = 0$, so it is a finite Galois extension. Case 1 implies

$$\mathbb{C} \subseteq F \subseteq F' = \mathbb{C}$$

so we have equality at each step. □

There are several important areas of Galois Theory that we do not have time to discuss. Here is a summary.

Galois Theory can be used to show that the general polynomial of degree 5 cannot be solved by radicals. Here is a sketch of how. There is a polynomial $f \in \mathbb{Q}[x]$ of degree 5 such that the splitting field $\mathbb{Q} \subseteq F$ has Galois group $\operatorname{Gal}(F : \mathbb{Q}) \cong S_5$. The group S_5 is not solvable. If f could be solved by radicals, then the Galois group $\operatorname{Gal}(F : \mathbb{Q})$ would necessarily be solvable.

Galois Theory can be used to show some theorems in geometry. For instance, there is not algorithm for trisecting an arbitrary angle using a ruler and compass. Specifically, the angle $60°$ cannot be trisected. If it could, then we could construct $\cos 20°$. If $\cos 20°$ could be constructed, then its minimal polynomial over $\mathbb{Q}$ would have to have degree equal to a power of 2. However, the minimal polynomial of $\cos 20°$ has degree 3. This idea can also be used to show that $\sqrt[3]{2}$ cannot be constructed using a ruler and compass, that is, one cannot duplicate a cube of side length 1.

Definition 21.2. Let K be a field and $f \in K[x]$ a polynomial. The *Galois group of f over K* is the group $\operatorname{Gal}(L : K)$ where L is a splitting field of f over K.

Another aspect of Galois Theory is the computation of Galois groups of certain classes of polynomials. We have dome some of this already. Other special cases are considered in Hungerford V.7–9.

CHAPTER 6

Module Theory II

1. Day 1

REMARK 1.1. Let R be a ring and let M and N be left R-modules. Recall that the set $\mathrm{Hom}_R(M,N)$ of all R-module homomorphisms $M \to N$ is an additive abelian group under pointwise addition $(f+g)(m) = f(m) + g(m)$. If R is commutative, then $\mathrm{Hom}_R(M,N)$ is a left R-module via the action $(rf)(m) = rf(m) = f(rm)$.

DEFINITION 1.2. Let R be a ring and let $\phi\colon M \to M'$ and $\psi\colon N \to N'$ be homomorphisms of left R-modules. Define the function

$$\mathrm{Hom}_R(M,\psi)\colon \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(M,N') \qquad \text{as} \qquad f \mapsto \psi \circ f.$$

Define the function

$$\mathrm{Hom}_R(\phi,N)\colon \mathrm{Hom}_R(M',N) \to \mathrm{Hom}_R(M,N) \qquad \text{as} \qquad g \mapsto g \circ \phi.$$

Let R-mod denote the category of left R-modules.

Recall that $\mathcal{A}b$ is the category of abelian groups.

PROPOSITION 1.3. *Let R be a ring and let M be a left R-module.*

(a) *The operator $\mathrm{Hom}_R(M,-)$ describes a covariant functor R-mod $\to \mathcal{A}b$. If R is commutative, then this describes a covariant functor R-mod $\to R$-mod.*
(b) *The operator $\mathrm{Hom}_R(-,M)$ describes a contravariant functor R-mod $\to \mathcal{A}b$. If R is commutative, then this operator describes a contravariant functor R-mod $\to R$-mod.*

PROOF. We will verify part (b). Part (a) is similar, and easier.

Using Remark 1.1, there are four things to show.

1. $\mathrm{Hom}_R(\phi,M)$ is a group homomorphism for each $\phi\colon N \to N'$: We need to show that

$$\mathrm{Hom}_R(\phi,M)(f+g) = \mathrm{Hom}_R(\phi,M)(f) + \mathrm{Hom}_R(\phi,M)(g)$$

for each $f, g \in \mathrm{Hom}_R(N',M)$. In other words, we need to show that

$$(f+g)\circ\phi = (f\circ\phi) + (g\circ\phi).$$

These are functions $N \to M$, so we check this on elements $m \in M$:

$$((f+g)\circ\phi)(m) = (f+g)(\phi(m)) = f(\phi(m)) + g(\phi(m)) = (f\circ\phi + g\circ\phi)(m)$$

2. $\mathrm{Hom}_R(\mathrm{id}_N,M) = \mathrm{id}_{\mathrm{Hom}_R(N,M)}$ for all N:

$$\mathrm{Hom}_R(\mathrm{id}_N,M)(g) = g \circ \mathrm{id}_N = g.$$

3. $\mathrm{Hom}_R(\phi \circ \psi, M) = \mathrm{Hom}_R(\psi, M) \circ \mathrm{Hom}_R(\phi, M)$:

$$\begin{aligned}\mathrm{Hom}_R(\phi \circ \psi, M)(g) &= g \circ (\phi \circ \psi) = (g \circ \phi) \circ \psi = \mathrm{Hom}_R(\psi, M)(g \circ \phi) \\ &= \mathrm{Hom}_R(\psi, M)(\mathrm{Hom}_R(\phi, M)(g)) \\ &= (\mathrm{Hom}_R(\psi, M) \circ \mathrm{Hom}_R(\phi, M))(g).\end{aligned}$$

4. Assuming that R is commutative, $\mathrm{Hom}_R(\phi, M)$ is an R-module homomorphism for each $\phi\colon N \to N'$: It remains to show that

$$\mathrm{Hom}_R(\phi, M)(rg) = r(\mathrm{Hom}_R(\phi, M)(g))$$

for each $r \in R$ and each $g \in \mathrm{Hom}_R(M', N)$. In other words, we need

$$(rg) \circ \phi = r(g \circ \phi).$$

As in part 1, we check this on elements $m \in M$:

$$((rg) \circ \phi)(m) = (rg)(\phi(m)) = r(g(\phi(m))) = (r(g \circ \phi))(m).$$

□

Proposition 1.4. *Let R be a ring and let $\phi\colon M \to M'$ be a homomorphism of left R-modules. Let $n \in \mathbb{N}$.*

(a) *$\mathrm{Hom}_R(R^n, M)$ is a left R-module by the action $(rf)(v) = f(vr)$. If R has identity, then this action is unital.*
(b) *The map $\mathrm{Hom}_R(R^n, \phi)\colon \mathrm{Hom}_R(R^n, M) \to \mathrm{Hom}_R(R^n, M')$ is a left R-module homomorphism.*
(c) *$\mathrm{Hom}_R(M, R^n)$ is a right R-module by the action $(\psi r)(v) = \phi(v)r$. If R has identity, then this action is unital.*
(d) *The map $\mathrm{Hom}_R(\phi, R^n)\colon \mathrm{Hom}_R(M', R^n) \to \mathrm{Hom}_R(M, R^n)$ is a right R-module homomorphism.*

Proof. We will prove parts (a) and (b). The other parts are proved similarly.

(a) We already know that $\mathrm{Hom}_R(R^n, M)$ is an additive abelian group. So, we have four things to check.

1. $r(f + g) = (rf) + (rg)$ for all $r \in R$ and all $f, g \in \mathrm{Hom}_R(R^n, M)$. We check this on elements $v \in R^n$:

$$(r(f + g))(v) = (f + g)(vr) = f(vr) + g(vr) = (rf)(v) + (rg)(v) = (rf + rg)(v).$$

2. $(r + s)f = (rf) + (sf)$ for all $r, s \in R$ and all $f \in \mathrm{Hom}_R(R^n, M)$. Check this on elements $v \in R^n$ as in part 1.

3. $(rs)f = r(sf)$ for all $r, s \in R$ and all $f \in \mathrm{Hom}_R(R^n, M)$. Check this on elements $v \in R^n$ as in part 1.

4. If R has identity, then $1f = f$ for all $f \in \mathrm{Hom}_R(R^n, M)$. Check this on elements $v \in R^n$ as in part 1.

(b) We need to check that $\mathrm{Hom}_R(R^n, \phi)(rf) = r(\mathrm{Hom}_R(R^n, \phi)(f))$ for all $r \in R$ and all $f \in \mathrm{Hom}_R(R^n, M)$. In other words, we need $\phi \circ (rf) = r(\phi f)$. We check this on elements $v \in R^n$:

$$(\phi \circ (rf))(v) = \phi((rf)(v)) = \phi(f(vr)) = (\phi f)(vr) = (r(\phi f))(v)$$

□

Proposition 1.5. *Let R be a ring with identity and let $\phi\colon M \to N$ be a homomorphism of unitary left R-modules. Let $n \in \mathbb{N}$ and let $e_1, \ldots, e_n \in R^n$ be a basis. Define $\Phi_M\colon \mathrm{Hom}_R(R^n, M) \to M^n$ by the formula $\Phi_M(f) = (f(e_1), \ldots, f(e_n))$.*

(a) *The map Φ_M is an isomorphism of left R-modules.*
(b) *There is a commutative diagram*

$$\begin{array}{ccc} \mathrm{Hom}_R(R^n, M) & \xrightarrow{\mathrm{Hom}_R(R^n,\phi)} & \mathrm{Hom}_R(R^n, N) \\ \Phi_M \downarrow \cong & & \Phi_N \downarrow \cong \\ M^n & \xrightarrow{\phi^n} & N^n \end{array}$$

where $\phi^n(m_1, \ldots, m_n) = (\phi(m_1), \ldots, \phi(m_n))$.

PROOF. (a) It is straightforward to show that Φ_M is an R-module homomorphism. To see that it is onto, let $(m_1, \ldots, m_n) \in M^n$. Proposition 4.2.4 says that the map $f\colon R^n \to M$ given by $f(r_1, \ldots, r_n) = \sum_i r_i m_i$ is a well-defined R-module homomorphism. By definition, we have $f(e_i) = m_i$ for each i, and so $\Phi_M(f) = (m_1, \ldots, m_n)$.

To see that Φ_M is 1-1, assume that $\Phi_M(f) = 0$. That is, $f(e_i) = 0$ for each i. It follows that for each $\sum_i r_i e_i \in R^n$, we have $f(\sum_i r_i e_i) = \sum_i r_i 0 = 0$. Thus $f = 0$ and Φ_M is bijective.

(b) For $\mathbf{f} \in \mathrm{Hom}_R(R^n, M)$, we compute:

$$\Phi_N(\mathrm{Hom}_R(R^n, \phi)(f)) = \Phi_N(\phi \circ f) = (\phi(f(e_1)), \ldots, \phi(f(e_n)))$$
$$\phi^n(\Phi_M(f)) = \phi^n(f(e_1), \ldots, f(e_n)) = (\phi(f(e_1)), \ldots, \phi(f(e_n)))$$

as desired. □

2. Day 2

The previous result says that the functors $(-)^n$ and $\mathrm{Hom}_R(R^n, -)$ are "naturally isomorphic".

DEFINITION 2.1. Let $\mathcal{C}$ and $\mathcal{D}$ be categories, and let $F, G\colon \mathcal{C} \to \mathcal{D}$ be covariant functors. A *natural transformation* from $T\colon F \to G$ is a function that assigns to each object C in $\mathcal{C}$ a morphism $T_C\colon F(C) \to G(C)$ in $\mathcal{D}$ such that, for every morphism $f\colon C \to C'$ in $\mathcal{C}$, the following diagram commutes:

$$\begin{array}{ccc} F(C) & \xrightarrow{F(f)} & F(C') \\ {\scriptstyle T_C}\downarrow & & \downarrow{\scriptstyle T_{C'}} \\ G(C) & \xrightarrow{G(f)} & G(C'). \end{array}$$

A natural transformation $T\colon F \to G$ is a *natural isomorphism* if, for every object C in $\mathcal{C}$, the map $T_C\colon F(C) \to G(C)$ is an isomorphism in $\mathcal{D}$.

DEFINITION 2.2. Let R be a ring. A sequence of left R-module homomorphisms

$$M_2 \xrightarrow{f_2} M_1 \xrightarrow{f_1} M_0$$

is *exact* if $\mathrm{Ker}(f_1) = \mathrm{Im}(f_2)$. More generally, a A sequence of left R-module homomorphisms

$$\cdots \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \cdots$$

is *exact* if $\mathrm{Ker}(f_i) = \mathrm{Im}(f_{i+1})$ for all i. A *short exact sequence* is an exact sequence of the form

$$0 \to M' \to M \to M'' \to 0.$$

REMARK 2.3. Given an sequence of left R-module homomorphisms

$$\cdots \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \cdots$$

we have $\operatorname{Ker}(f_i) \supseteq \operatorname{Im}(f_{i+1})$ if and only if $f_i f_{i+1} = 0$.

EXAMPLE 2.4. Let M', M'' be left R-modules. Then the sequence

$$0 \to M' \xrightarrow{f} M' \oplus M'' \xrightarrow{g} M'' \to 0$$

is exact. Here $f(m') = (m', 0)$ and $g(m', m'') = m''$.

EXAMPLE 2.5. Let R be a ring and let $I \subseteq R$ be an ideal. Then the sequence

$$0 \to I \xrightarrow{f} R \xrightarrow{g} R/I \to 0$$

is exact. Here f is the inclusion and g is the natural surjection.

More generally, let M be a left R-module, and let $M' \subseteq M$ be submodule. Then the sequence

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M/M' \to 0$$

is exact. Here f is the inclusion and g is the natural surjection.

PROPOSITION 2.6. *Let R be a ring.*

(a) *The sequence $0 \to M' \xrightarrow{f} M$ is exact if and only if f is 1-1.*
(b) *The sequence $M \xrightarrow{g} M'' \to 0$ is exact if and only if g is onto.*

PROOF. f is 1-1 if and only if $\operatorname{Ker}(f) = 0 = \operatorname{Im}(0 \to M')$. g is onto if and only if $\operatorname{Im}(g) = M'' = \operatorname{Ker}(M'' \to 0)$. □

DEFINITION 2.7. Let R be a ring, and consider two exact sequence of left R-module homomorphisms

$$M_\bullet = \cdots \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \cdots$$

and

$$N_\bullet = \cdots \xrightarrow{g_{i+1}} N_i \xrightarrow{g_i} N_{i-1} \xrightarrow{g_{i-1}} \cdots .$$

A *homomorphism* from $M_\bullet$ to $N_\bullet$ is a sequence of maps $h_\bullet = \{h_n \colon M_n \to N_n \mid n \in \mathbb{Z}\}$ such that $h_{n-1} f_n = g_n h_n$ for all $n \in \mathbb{Z}$. In other words, the maps h_n make the following "ladder diagram" commute.

$$\begin{array}{ccccccccc}
M_\bullet & & \cdots & \xrightarrow{f_{i+1}} & M_i & \xrightarrow{f_i} & M_{i-1} & \xrightarrow{f_{i-1}} & \cdots \\
{\scriptstyle h_\bullet}\downarrow & & & & \downarrow{\scriptstyle h_i} & & \downarrow{\scriptstyle h_{i-1}} & & \\
N_\bullet & & \cdots & \xrightarrow{g_{i+1}} & N_i & \xrightarrow{g_i} & N_{i-1} & \xrightarrow{g_{i-1}} & \cdots .
\end{array}$$

The homomorphism $h_\bullet$ is an *isomorphism* from $M_\bullet$ to $N_\bullet$ if it has a two-sided inverse, that is, if there exists a homomorphism $k_\bullet \colon N_\bullet \to M_\bullet$ such that $h_n k_n = \mathrm{id}_{N_n}$ and $k_n h_n = \mathrm{id}_{M_n}$ for all n.

REMARK 2.8. Let R be a ring, and consider two exact sequence of left R-module homomorphisms

$$M_\bullet = \cdots \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \cdots$$
$$N_\bullet = \cdots \xrightarrow{g_{i+1}} N_i \xrightarrow{g_i} N_{i-1} \xrightarrow{g_{i-1}} \cdots .$$

Let $h_\bullet \colon M_\bullet \to N_\bullet$ be a homomorphism of exact sequences. Show that $h_\bullet$ is an isomorphism if and only if each h_n is an isomorphism.

EXAMPLE 2.9. Given two integers m and n with $n \neq 0$, here is a homomorphism of short exact sequences of abelian groups:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle n} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & n\mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0. \end{array}$$

Here the unlabeled maps are the natural inclusions and surjections. This homomorphism is an isomorphism if and only if $m = 0$.

3. Day 3

PROPOSITION 3.1 (Short Five Lemma). *Let R be a ring, and consider a homomorphism of exact sequences*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle k} & & \downarrow{\scriptstyle l} & & \\ 0 & \longrightarrow & N' & \xrightarrow{F} & N & \xrightarrow{G} & N'' & \longrightarrow & 0 \end{array}$$

(a) *If h and l are 1-1, then k is 1-1.*
(b) *If h and l are onto, then k is onto.*

PROOF. (a) Assume that h and l are 1-1. Let $m \in \mathrm{Ker}(k) \subseteq M$. Commutativity of the diagram implies that

$$l(g(m)) = G(k(m)) = G(0) = 0.$$

Since l is 1-1, we have $g(m) = 0$. The exactness of the top row of the diagram implies that $m \in \mathrm{Ker}(g) = \mathrm{Im}(f)$ and so $m = f(m')$ for some $m' \in M'$. It follows that

$$0 = k(m) = k(f(m')) = F(h(m')).$$

Since F and h are 1-1, it follows that $m' = 0$ and so $m = f(m') = f(0) = 0$.

(b) Assume that h and l are onto. Let $n \in N$. Since l is onto, there exists $m'' \in M''$ such that $l(m'') = G(n)$. Since g is onto, there exists $m \in M$ such that $g(m) = m''$, and so

$$G(k(m)) = l(g(m)) = l(m'') = G(n).$$

(We would like to conclude that $k(m) = n$, but this may not be true.) Instead, the displayed equation implies that $G(k(m) - n) = G(k(m)) - G(n) = 0$ and so $k(m) - n \in \mathrm{Ker}(G) = \mathrm{Im}(F)$. Write $k(m) - n = F(n')$ for some $n' \in N'$. Since h is onto, there exists $m' \in M'$ such that $h(m') = n'$. It follows that

$$k(f(m')) = F(h(m')) = F(n') = k(m) - n$$

and so$k(m - f(m')) = n$. Thus, $n \in \mathrm{Im}(k)$ and so k is onto. □

DEFINITION 3.2. Let R be a ring. An exact sequence

$$0 \to M' \to M \to M'' \to 0$$

is *split* if it is isomorphic to the sequence

$$0 \to M' \xrightarrow{f} M' \oplus M'' \xrightarrow{g} M'' \to 0$$

where $f(m') = (m', 0)$ and $g(m', m'') = m''$. In particular, if the given sequence is split, then $M \cong M' \oplus M''$.

Here is a classification of split exact sequences.

PROPOSITION 3.3. *Let R be a ring, and consider an exact sequence*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0.$$

TFAE.

(i) *The exact sequence is split;*
(ii) *There is an R-module homomorphism $f_1 \colon M \to M'$ such that $f_1 \circ f = \mathrm{id}_{M'}$;*
(iii) *There is an R-module homomorphism $g_1 \colon M'' \to M$ such that $g \circ g_1 = \mathrm{id}_{M''}$.*

PROOF. We will prove (i) $\iff$ (ii). The proof of (i) $\iff$ (iii) is similar.

(i) $\implies$ (ii) Assume that the given sequence is split. Then there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle h}\cong & & \downarrow{\scriptstyle k}\cong & & \downarrow{\scriptstyle l}\cong & & \\ 0 & \longrightarrow & M' & \xrightarrow{i} & M' \oplus M'' & \xrightarrow{t} & M'' & \longrightarrow & 0 \end{array}$$

where $i(m') = (m', 0)$ and $t(m', m'') = m''$. Let $i_1 \colon M' \oplus M'' \to M'$ be given by $i_1(m', m'') = m'$. We will show that the map $f_1 = h^{-1} \circ i_1 \circ k \colon M \to M'$ satisfies the desired property.

We first compute:

$$i \circ h \circ f_1 \circ f = i \circ h \circ h^{-1} \circ i_1 \circ k \circ f = i \circ i_1 \circ k \circ f = i \circ i_1 \circ i \circ h = i \circ \mathrm{id}_{M'} \circ h = i \circ h.$$

The third equality follows from the commutativity of the diagram. The remaining equalities are by definition. Thus, we have

$$(i \circ h) \circ (f_1 \circ f) = i \circ h = (i \circ h) \circ \mathrm{id}_{M'}.$$

Since i and h are 1-1, it follows that $f_1 \circ f = \mathrm{id}_{M'}$ as desired.

(i) $\impliedby$ (ii) Assume that there is an R-module homomorphism $f_1 \colon M \to M'$ such that $f_1 \circ f = \mathrm{id}_{M'}$. Let $F \colon M \to M' \oplus M''$ be given by $F(m) = (f_1(m), g(m))$. We will show that the following diagram commutes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{M'}}\cong & & \downarrow{\scriptstyle F}\cong & & \downarrow{\scriptstyle \mathrm{id}_{M''}}\cong & & \\ 0 & \longrightarrow & M' & \xrightarrow{i} & M' \oplus M'' & \xrightarrow{t} & M'' & \longrightarrow & 0 \end{array}$$

where $i(m') = (m', 0)$ and $t(m', m'') = m''$. The Short Five Lemma will then imply that F is an isomorphism, so that the displayed diagram is an isomorphism of exact sequences; by definition, it then follows that the original sequence is split.

We compute: for $m' \in M'$ and $m \in M$ we have

$$F(f(m')) = (f_1(f(m')), g(f(m'))) = (m', 0) = i(m').$$

$$t(F(m)) = t(f_1(m), g(m)) = g(m).$$

□

COROLLARY 3.4. *Let R be a ring with identity, and consider an exact sequence*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

of unitary R-modules. If M'' is free, then this sequence is split.

PROOF. It suffices to find an R-module homomorphism $g_1 \colon M'' \to M$ such that $gg_1 = \mathrm{id}_{M''}$. Since M'' is free, it has a basis $B \subseteq M''$. g is surjective, so for each $b \in B$, there exists $m_b \in M$ such that $g(m_b) = b$. Define $g_1 \colon M'' \to M$ by the formula $g_1(\sum_b a_b b) = \sum_b a_b m_b$. Proposition 4.2.4 says that f_1 is a well-defined R-module homomorphism. We compute:

$$g(g_1(\textstyle\sum_b a_b b)) = g(\sum_b a_b m_b) = \sum_b a_b g(m_b) = \sum_b a_b b$$

which shows that $g \circ g_1 = \mathrm{id}_{M''}$, as desired. □

COROLLARY 3.5. *Let R be a ring with identity, and consider an exact sequence*

$$0 \to R^m \xrightarrow{f} R^n \xrightarrow{g} R^p \to 0.$$

Then $n = m + p$.

PROOF. Corollary 3.4 implies that the given sequence splits. In particular, we have $R^n \cong R^m \oplus R^p \cong R^{m+p}$. The invariant basis property implies that $n = m + p$. □

4. Day 4

DEFINITION 4.1. Let R be a ring. A left R-module M is *noetherian* if it satisfies the *ascending chain condition (ACC) on submodules*: For every ascending chain of submodules $M_1 \subseteq M_2 \subseteq \cdots \subseteq M$, we have $M_n = M_{n+1} = M_{n+2} = \cdots$ for some $n \geqslant 1$.

Slogan: every ascending chain of submodules stabilizes.

The ring R is *(left) noetherian* if it is noetherian as an R-module, that is, if it satisfies ACC on left ideals.

EXAMPLE 4.2. Every field k is a noetherian ring because the only ideals are (0) and k. More generally, every PID is noetherian by Lemma 3.8.2.

THEOREM 4.3. *Let R be a ring and M an R-module. The following conditions are equivalent:*

(i) *M is noetherian as an R-module;*
(ii) *every left submodule of M is finitely generated;*
(iii) *every nonempty set of left submodules of M has a maximal element.*

PROOF. (i) $\implies$ (ii). Assume that M is noetherian and let $N \subseteq M$ be a left submodule. Suppose that N is not finitely generated. In particular, we have $N \neq (0)$. Let $0 \neq x_1 \in N$. Since N is not finitely generated, we have $(x_1) \subsetneq N$, so we have $x_2 \in N - (x_1)$. It follows that $(x_1) \subsetneq (x_1, x_2)$ because $x_2 \in (x_1, x_2) - (x_1)$. Since N is not finitely generated, we have $(x_1, x_2) \subsetneq N$, so we have $x_3 \in N - (x_1, x_2)$. It follows that $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3)$ because $x_3 \in (x_1, x_2, x_3) - (x_1, x_2)$. Continue inductively to find construct an ascending chain of left submodules

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots \subsetneq (x_1, x_2, \ldots, x_n) \subsetneq (x_1, x_2, \ldots, x_n, x_{n+1}) \subsetneq \cdots$$

This chain never stabilizes, contradicting our noetherian assumption. Thus, N is finitely generated.

(ii) $\Longrightarrow$ (iii). Assume that every left submodule of M is finitely generated, and let S be a nonempty set of left submodules of M. We need to show that S has a maximal element N, that is, a submodule N in S with the following property: If P is a submodule in S such that $N \subseteq P$, then $N = P$.

We employ Zorn's Lemma. For this, we need to show that every chain in S has an upper bound in S. Let C be a chain of submodules in S. As usual the union $N = \cup_{P \in C} P$ is a left submodule of R. We need to show that N is in S. By assumption, the submodule N is finitely generated, say $N = (a_1, \ldots, a_n)$. Since each $a_i \in N = \cup_{P \in C} P$, we have $a_i \in P_i$ for some $P_i \in C$. Since C is a chain, there is an index j such that $P_i \subseteq P_j$ for each i. Hence, we have $a_i \in P_j$ for each i, and so

$$N = (a_1, \ldots, a_n) \subseteq P_j \subseteq N.$$

It follows that $N = P_j \in S$, as desired.

(iii) $\Longrightarrow$ (i). Assume every nonempty set of left submodules of M has a maximal element, and consider a chain of left submodules $M_1 \subseteq M_2 \subseteq \cdots \subseteq M$. We need to show that the chain stabilizes. By assumption, the set $S = \{M_1, M_2, \ldots\}$ has a maximal element, say it is M_n. For each $i \geqslant 1$ we have $M_n \subseteq M_{n+i}$, so the maximality of M_n implies $M_n = M_{n+i}$. Thus, the chain stabilizes and M is noetherian. □

COROLLARY 4.4. *Let R be a ring. The following conditions are equivalent:*

(i) *R is noetherian;*
(ii) *every left ideal of R is finitely generated;*
(iii) *every nonempty set of left ideals of R has a maximal element.*

PROOF. This is the special case $M = R$ of Theorem 4.3. □

This characterization shows how to construct a ring that is not noetherian.

EXAMPLE 4.5. Let k be a field and let $R = k[x_1, x_2, \ldots]$ be a polynomial ring in infinitely many variables. The ideal $(x_1, x_2, \ldots) \subset R$ is not finitely generated and so R is not noetherian.

THEOREM 4.6 (Hilbert Basis Theorem). *Let R be a commutative ring with identity. The polynomial ring $R[x]$ is noetherian.*

PROOF. Let $I \subseteq R[x]$ be an ideal. We will show that I is finitely generated.

For each $r = 0, 1, 2, \ldots$ let

$$I_r = \{a \in R \mid \exists a_0 + a_1 x + \ldots + a_{r-1} x^{r-1} + a x^r \in I\}.$$

Since I is an ideal in $R[x]$, it follows readily that I_r is an ideal in R. Furthermore, we have $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq R$: If $a \in I_r$ then there exists a polynomial $f = a_0 + a_1 x + \ldots + a_{r-1} x^{r-1} + a x^r \in I$; since I is an ideal the polynomial $xf = a_0 x + a_1 x^2 + \ldots + a_{r-1} x^r + a x^{r+1} \in I$, and so $a \in I_{r+1}$.

Since R is noetherian, there exists $J \geqslant 0$ such that, for every $j \geqslant J$ we have $I_j = I_J$. Furthermore, every I_r is finitely generated, say, $I_r = (a_{r,1}, \ldots, a_{r,k_r})$. Thus, there exist $f_{r,1}, \ldots, f_{r,k_r} \in I$ such that $f_{r,i} = a_{r,i,0} + a_{r,i,1} x + \ldots + a_{r,i,r-1} x^{r-1} + a_{r,i} x^r$.

Claim: $I = (\{f_{r,i} \mid r = 0, \ldots, J;\ i = 1, \ldots, k_r\})$. (Once this is proved, we are done.) Set $I' = (\{f_{r,i} \mid r = 0, \ldots, J;\ i = 1, \ldots, k_r\})$. The containment $I \supseteq I'$ holds because each $f_{r,i} \in I$. for the containment $I \subseteq I'$, let $f \in I$. Since $0 \in I'$, we assume that $f \neq 0$ and set $s = \deg(f)$. We show that $f \in I'$ by induction on s.

Base case: $s = 0$. Here we see that f is constant, and so $f = a_0 \in R$. Since $f \in I$, we conclude that $f \in I_0 = (a_{0,1}, \ldots, a_{0,k_0}) = (f_{0,1}, \ldots, f_{0,k_0}) \subseteq I'$.

Inductive step: Assume that $s \geqslant 1$ and that, for every polynomial $g \in I$ with $\deg(g) < s$, we have $g \in I'$. Write $f = b_0 + \cdots + b_s x^s$.

Case 1: $s \leqslant J$. Then $b_s \in I_s = (a_{s,1}, \ldots, a_{s,k_s})$. Write $b_s = \sum_{i=1}^{k_s} c_i a_{s,i}$ with each $c_i \in R$. The polynomial $g = f - \sum_{i=1}^{k_s} c_i f_{s,i} x^{r-s} \in I$ is either 0 or has $\deg(g) < s$. Furthermore, we have $f - g = \sum_{i=1}^{k_s} c_i f_{s,i} x^{r-s} \in (f_{s,1}, \ldots, f_{s,k_s}) \subseteq I'$, and so $f \in I'$ if and only if $g \in I'$. By our induction hypothesis, we have $g \in I'$, and so $f \in I'$, as desired.

Case 2: $s > J$. Then $b_s \in I_s = I_J = (a_{J,1}, \ldots, a_{J,k_J})$. Write $b_s = \sum_{i=1}^{k_J} c_i a_{J,i}$ with each $c_i \in R$. The polynomial $g = f - \sum_{i=1}^{k_J} c_i f_{J,i} x^{r-J} \in I$ is either 0 or has $\deg(g) < s$. Furthermore, we have $f - g = \sum_{i=1}^{k_J} c_i f_{J,i} x^{r-J} \in I'$, and so $f \in I'$ if and only if $g \in I'$. By our induction hypothesis, we have $g \in I'$, and so $f \in I'$, as desired. □

5. Day 5

The Hilbert Basis Theorem gives a lot of examples of noetherian rings.

COROLLARY 5.1. *Let R be a commutative ring with identity. Every finitely generated R-algebra is noetherian. In particular, each polynomial ring in finitely many variables $R[x_1, \ldots, x_n]$ is noetherian.*

PROOF. For polynomial rings, the result follows from the Hilbert Basis Theorem by induction on the number of variables. In general, each finitely generated R-algebra is (isomorphic to a ring) of the form $R[x_1, \ldots, x_n]/J$. Since R is noetherian, the same is true of the polynomial ring $R[x_1, \ldots, x_n]$, and an exercise shows that the same is true for the quotient $R[x_1, \ldots, x_n]/J$. □

THEOREM 5.2. *Let R be a ring and consider an exact sequence of R-modules:*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0.$$

Then M is noetherian if and only if M' and M'' are noetherian.

PROOF. Assume that M' and M'' are noetherian. To see that M is noetherian, consider an ascending chain $M_1 \subseteq M_2 \subseteq \cdots \subseteq M$. Since M' is noetherian, the ascending chain $f^{-1}(M_1) \subseteq f^{-1}(M_2) \subseteq \cdots \subseteq M'$ stabilizes. Since M'' is noetherian, the ascending chain $g(M_1) \subseteq g(M_2) \subseteq \cdots \subseteq M''$ stabilizes. Thus, there exists $n \geqslant 1$ such that $f^{-1}(M_n) = f^{-1}(M_{n+1}) = \cdots$ and $g(M_n) = g(M_{n+1}) = \cdots$.

We show that $M_n = M_{n+1} = \cdots$. For this, it suffices to show that $M_{n+i} \subseteq M_n$ for each $i \geqslant 1$. Let $m \in M_{n+i}$. Then $g(m) \in g(M_{n+i}) = g(M_n)$, so there exists $m_1 \in M_n$ such that $g(m_1) = g(m)$. Then $m - m_1 \in \operatorname{Ker}(g) = \operatorname{Im}(f)$, so there exists $m' \in M'$ such that $g(m') = m - m_1$. Note that $m \in M_{n+i}$ and $m_1 \in M_n \subseteq M_{n+i}$, and so $m - m_1 \in M_{n+i}$. It follows that $m' \in f^{-1}(M_{n+i}) = f^{-1}(M_n)$. Hence, we have $m - m_1 = f(m') \in M_n$ and so $m = m_1 + f(m') \in M_n$, as desired.

The converse is an exercise. □

THEOREM 5.3. *Let R be a ring with identity. Then R is a noetherian ring if and only if every finitely generated R-module is noetherian.*

PROOF. If every finitely generated R-module is noetherian, then the R-module R is noetherian; that is, R is a noetherian ring.

Conversely, assume that R is a noetherian ring. For each $n \geqslant 0$, the module R^n is noetherian. This is true for $n = 0, 1$ by hypothesis. For $n \geqslant 2$, use induction applied to the exact sequence

$$0 \to R \to R^n \to R^{n-1} \to 0$$

along with Theorem 5.2.

Now let M be a finitely generated R-module. Then there is an integer $n \geqslant 0$ and an epimorphism $\tau\colon R^n \to M$. Since R^n is noetherian, Theorem 5.2 shows that $M \cong R^n/\operatorname{Ker}(\tau)$ is also noetherian. □

The next result compares to Proposition 1.20.2.

PROPOSITION 5.4. *Let R be a PID. Every submodule of R^n is free of rank $\leqslant n$.*

PROOF. By induction on n. If $n = 1$, then every submodule $M \subseteq R$ is $M = rR$ for some $r \in R$. Therefore,

$$M = \begin{cases} \{0\} \cong R^0 & \text{if } r = 0 \\ rR \cong R^1 & \text{if } r \neq 0. \end{cases}$$

Assume $n > 1$ and assume that every submodule of R^{n-1} is free of rank $\leqslant n-1$. Let $K \subseteq R^n$ be a submodule, and define $t\colon R^n \to R$ by the formula $t(a_1, \ldots, a_n) = a_n$. Check that t is a homomorphism with $\operatorname{Ker}(t) = R^{n-1} \oplus \{0\} \cong R^{n-1}$. It follows that $t(K) \subseteq R$, so $t(K) = rR$ for some $r \in R$. If $r = 0$, then $K \subseteq \operatorname{Ker}(t) = R^{n-1}$, so our induction hypothesis implies that K is free of rank $\leqslant n - 1$. So, we assume that $r \neq 0$.

Define $g\colon K \to t(K)$ by the formula $g(k) = t(k)$. Then g is an R-module epimorphism. It is straightforward to verify that

$$\operatorname{Ker}(g) = \operatorname{Ker}(t) \cap K = R^{n-1} \cap K \subseteq R^{n-1}.$$

By our induction hypothesis, we have $\operatorname{Ker}(g) \cong R^m$ for some $m \leqslant n - 1$.

There is an exact sequence

$$0 \to \operatorname{Ker}(g) \to K \xrightarrow{g} t(K) \to 0.$$

Since $t(K)$ is free, this sequence splits, so we have

$$K \cong \operatorname{Ker}(g) \oplus t(K) \cong R^m \oplus R \cong R^{m+1}.$$

Since $m + 1 \leqslant n$, this is the desired result. □

The next discussion compares to Remark 1.21.1.

REMARK 5.5. Let R be a commutative ring with identity, and fix integers $n, k \geqslant 1$. Recall that we have $\operatorname{Hom}_R(R^k, R^n) \cong \mathcal{M}_{n\times k}(R)$. Specifically, let $h\colon R^k \to R^n$ be an R-module homomorphism. Write elements of R^k and R^n as column vectors with entries in R. Let $\mathbf{e}_1, \ldots, \mathbf{e}_k \in R^k$ be the standard basis. For $j = 1, \ldots, k$ write

$$h(\mathbf{e}_j) = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{i,j} \\ \vdots \\ a_{n,j} \end{pmatrix}.$$

Then h is represented by the $n \times k$ matrix

$$[f] = (a_{i,j}) = \begin{pmatrix} a_{1,1} & \cdots & a_{1,j} & \cdots & a_{1,k} \\ \vdots & & \vdots & & \vdots \\ a_{i,1} & \cdots & a_{i,j} & \cdots & a_{i,k} \\ \vdots & & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,j} & \cdots & a_{n,k} \end{pmatrix}$$

in the following sense: For each vector

$$\begin{pmatrix} r_1 \\ \vdots \\ r_k \end{pmatrix} \in R^k$$

we have

$$h \begin{pmatrix} r_1 \\ \vdots \\ r_k \end{pmatrix} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,k} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,k} \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_k \end{pmatrix}.$$

We have elementary basis operations on the $\mathbf{e}_j$:

(1) Replace $\mathbf{e}_j$ with $u\mathbf{e}_j$ where $u \in R$ is a unit;
(2) Interchange $\mathbf{e}_j$ and $\mathbf{e}_l$;
(3) Replace $\mathbf{e}_j$ with $\mathbf{e}_j + r\mathbf{e}_l$ for some $r \in R$ and $l \neq j$.

These correspond to the appropriate elementary column operations on the matrix $(a_{i,j})$, in the following sense. Applying one of the elementary basis operations to the $\mathbf{e}_j$ yields an isomorphism $\Phi\colon R^k \to R^k$ such that the following diagram commutes

$$\begin{array}{ccc} R^k & \xrightarrow{(a_{i,j})} & R^n \\ {\scriptstyle\Phi}\downarrow{\scriptstyle\cong} & & \downarrow{=} \\ R^k & \xrightarrow{(b_{i,j})} & R^n \end{array}$$

where $(b_{i,j})$ is the matrix obtained by applying the corresponding elementary column operation to the matrix $(a_{i,j})$. And, conversely, if $(b_{i,j})$ is obtained from $(a_{i,j})$ by an elementary column operation, then the corresponding elementary basis operations on the $\mathbf{e}_j$ yields a commutative diagram as above.

Let $\mathbf{f}_1, \ldots, \mathbf{f}_n \in R^n$ be the standard basis. The elementary basis operations on the $\mathbf{f}_j$ correspond similarly to the elementary row operations on the matrix $(a_{i,j})$.

Furthermore, if we repeatedly apply elementary row and column operations to the matrix $(a_{i,j})$ to obtain the matrix $(c_{i,j})$, then this yields a commutative diagram

$$\begin{array}{ccc} R^k & \xrightarrow{(a_{i,j})} & R^n \\ {\scriptstyle\Phi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\Psi}\downarrow{\scriptstyle\cong} \\ R^k & \xrightarrow{(c_{i,j})} & R^n. \end{array}$$

We say that an $n \times k$ matrix $(d_{i,j})$ with entries in R is *equivalent* to $(a_{i,j})$ if it can be obtained from $(a_{i,j})$ using a (finite) sequence of elementary row and column operations.

6. Day 6

The next result compares to Proposition 1.21.2.

PROPOSITION 6.1. *Let R be a PID. Fix integers $n \geqslant k \geqslant 1$ and let $h\colon R^k \to R^n$ be an R-module monomorphism. There exists a commutative diagram of group homomorphisms*

$$\begin{array}{ccc} R^k & \xrightarrow{h} & R^n \\ {\scriptstyle\Phi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\Psi}\downarrow{\scriptstyle\cong} \\ R^k & \xrightarrow{h'} & R^n \end{array}$$

such that the matrix representing h' is "diagonal", that is, $[h'] = (d_{i,j})$ where $d_{i,j} = 0$ when $i \neq j$.

PROOF. Let $[h] = (a_{i,j})$, and let A denote the set of all $s \in R$ such that a finite number of elementary row and column operations applied to $(a_{i,j})$ yields a matrix with s in the upper left corner. The set $S = \{sR \mid s \in A\}$ is a nonempty set of ideals of R. Since R is a PID, it is noetherian, and so S has a maximal element. Apply the necessary row and column operations to yield a new matrix $(b_{i,j})$ such that $b_{1,1}R$ is a maximal element of S.

Note that $b_{1,1} \neq 0$. Indeed, since h is a monomorphism, the matrix $(b_{i,j})$ is nonzero. It follows that a finite number of row and column operations will yield a matrix with a nonzero element $s \neq 0$ in the upper left corner. If $b_{1,1} = 0$, then $b_{1,1}R = (0) \subsetneq sR$, contradicting the maximality of $b_{1,1}$ in S.

Claim: $b_{1,1} \big| b_{1,2}$. Suppose not. Then $b_{1,2} \notin b_{1,1}R$. It follows that $b_{1,1}R \subsetneq (b_{1,1}, b_{1,2})R$. Since R is a PID, there is an element $d \in R$ such that $(b_{1,1}, b_{1,2})R = dR$. Thus, we have

$$(0) \subsetneq b_{1,1}R \subsetneq (b_{1,1}, b_{1,2})R = dR.$$

In particular, we have $d \neq 0$. We will derive a contradiction by showing that $d \in A$; the relation $b_{1,1}R \subsetneq dR$ will then contradict the maximality of $b_{1,1}R$ in S.

Since $d \in dR = (b_{1,1}, b_{1,2})R$, there are elements $u, v \in R$ such that $d = ub_{1,1} + vb_{1,2}$. On the other hand, we have $b_{1,1}, b_{1,2} \in (b_{1,1}, b_{1,2})R = dR$ and so there are elements $x, y \in R$ such that $b_{1,1} = xd$ and $b_{1,2} = yd$. This yields

$$1d = d = ub_{1,1} + vb_{1,2} = uxd + vyd = (ux + vy)d$$

and so $ux + vy = 1$ because $d \neq 0$.

Consider the following matrix multiplication:

$$\begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,k} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,k} \\ \vdots & \vdots & & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,k} \end{pmatrix} \begin{pmatrix} u & -y & 0 & \cdots & 0 \\ v & x & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} d & * & \cdots & * \\ * & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ * & * & \cdots & * \end{pmatrix}$$

Because $ux + vy = 1$, it can be shown that the second matrix corresponds to a change of basis. It follows that $d \in A$, as desired.

A similar argument shows that $b_{1,1} \big| b_{1,i}$ for $i = 2, \ldots, k$ and $b_{1,1} \big| b_{j,1}$ for $j = 2, \ldots, n$. Thus, we may use elementary row and column operations to find an matrix $(c_{i,j})$ equivalent to $(b_{i,j})$ and hence equivalent to $(a_{i,j})$ such that $r \neq 1$ implies $c_{1,r} = 0$ and $c_{r,1} = 0$:

$$\begin{pmatrix} c_{1,1} & 0 & 0 & \cdots & 0 \\ 0 & c_{2,2} & c_{2,3} & \cdots & c_{2,k} \\ 0 & c_{3,2} & c_{3,3} & \cdots & c_{3,k} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & c_{n,2} & c_{n,3} & \cdots & c_{n,k} \end{pmatrix}$$

Repeating this process to appropriate "submatrices" of $(c_{i,j})$ yields the desired matrix, and Remark 5.5 yields the desired commutative diagram. □

The next result compares to Proposition 1.21.3.

PROPOSITION 6.2. *Let R be a ring, and let $h\colon K \to N$ and $h'\colon K' \to N'$ be R-module homomorphisms. Given a commutative diagram of R-module homomorphisms*

$$\begin{array}{ccc} K & \xrightarrow{h} & N \\ {\scriptstyle\Phi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\Psi}\downarrow{\scriptstyle\cong} \\ K' & \xrightarrow{h'} & N' \end{array}$$

there is an R-module isomorphism $\alpha\colon N/\operatorname{Im}(h) \xrightarrow{\cong} N'/\operatorname{Im}(h')$.

PROOF. Let $\alpha\colon N/\operatorname{Im}(h) \to N'/\operatorname{Im}(h')$ be given by $\alpha(\overline{x}) = \overline{\Psi(x)}$. Proposition 1.21.3 shows that α is a well-defined abelian group isomorphism. From the definition, it is straightforward to show that α is an R-module homomorphism. □

Here is the Fundamental Theorem for Finitely Generated Modules over a PID. Compare to Theorem 1.22.1.

THEOREM 6.3. *Let R be a PID and let M be a finitely generated R-modle. Then G is a direct sum of cyclic R-modules:*

$$M \cong R/d_1R \oplus \cdots \oplus R/d_kR \oplus R^{n-k}.$$

PROOF. Let $\{m_1, \ldots, m_n\} \subseteq M$ be a generating set for M. The map $f\colon R^n \to M$ given by $f(r_1, \ldots, r_n) = \sum_i r_i m_i$ is a well-defined group epimorphism. We have $\operatorname{Ker}(f) \subseteq R^n$, so Proposition 5.4 yields an isomorphism $h_1\colon R^k \xrightarrow{\cong} \operatorname{Ker}(f)$ for some $k \leqslant n$. Let $\varepsilon\colon \operatorname{Ker}(f) \to R^n$ be the natural inclusion, and set $h = \varepsilon h_1\colon R^k \to R^n$. Since h_1 is an isomorphism and ε is a monomorphism, we know that h is a monomorphism.

Proposition 6.1 yields a commutative diagram of group homomorphisms

$$\begin{array}{ccc} R^k & \xrightarrow{h} & R^n \\ {\scriptstyle\Phi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\Psi}\downarrow{\scriptstyle\cong} \\ R^k & \xrightarrow{h'} & R^n \end{array}$$

such that $[h'] = (d_{i,j})$ where $d_{i,j} = 0$ when $i \neq j$. Let $\mathbf{f}_1, \ldots, \mathbf{f}_n \in \mathbb{Z}^n$ be the standard basis. Then we have

$$\begin{aligned} M &\cong R^n/\operatorname{Ker}(f) && \text{first isomorphism theorem} \\ &= R^n/\operatorname{Im}(h) && \text{construction of } h \\ &\cong R^n/\operatorname{Im}(h') && \text{Proposition 6.2} \\ &= R^n/\langle d_{1,1}\mathbf{f}_1, \ldots, d_{k,k}\mathbf{f}_k\rangle && \text{assumptions on } h' \\ &\cong R/d_{1,1}R \oplus \cdots \oplus R/d_{k,k}R \oplus \mathbb{Z}^{n-k} && \text{Exercise.} \end{aligned}$$

This is the desired conclusion. □

DEFINITION 6.4. Let R be a ring and let $F\colon R\text{-mod} \to \mathcal{A}b$ be a covariant functor. The functor F is *additive* if, for each pair of R-module homomorphisms $f, g\colon M \to N$, we have

$$F(f+g) = F(f) + F(g)\colon F(M) \to F(N).$$

In other words, F is additive if, for every pair of R-modules, the map

$$F_{M,N}\colon \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_{\mathcal{A}b}(F(M), F(N))$$

is an abelian group homomorphism.

Let $G\colon R\text{-mod} \to \mathcal{A}b$ be a contravariant functor. The functor G is *additive* if, for each pair of R-module homomorphisms $f, g\colon M \to N$, we have

$$G(f+g) = G(f) + G(g)\colon G(N) \to G(M).$$

In other words, G is additive if, for every pair of R-modules, the map

$$G_{M,N}\colon \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_{\mathcal{A}b}(G(N), G(M))$$

is an abelian group homomorphism.

REMARK 6.5. Let R be a ring and let $F\colon R\text{-mod} \to \mathcal{A}b$ be a functor, either covariant or contravariant. Then $F(0) = 0$.

EXAMPLE 6.6. Let R be a ring and let M be an R-module. The functor $\operatorname{Hom}_R(M, -)$ is covariant and additive. The functor $\operatorname{Hom}_R(-, M)$ is contravariant and additive.

7. Day 7

DEFINITION 7.1. Let R be a ring and let $F\colon R\text{-mod} \to \mathcal{A}b$ be a covariant additive functor.

The functor F is *exact* if, for every exact sequence

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

the induced sequence

$$F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'')$$

is also exact.

The functor F is *left exact* if, for every exact sequence

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M''$$

the induced sequence

$$0 \to F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'')$$

is also exact.

The functor F is *right exact* if, for every exact sequence

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

the induced sequence

$$F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'') \to 0$$

is also exact.

Let $G\colon R\text{-mod} \to \mathcal{A}b$ be a contravariant additive functor.

The functor G is *exact* if, for every exact sequence

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

the induced sequence

$$G(M'') \xrightarrow{G(g)} G(M) \xrightarrow{G(f)} G(M')$$

is also exact.

The functor G is *left exact* if, for every exact sequence

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

the induced sequence

$$0 \to G(M'') \xrightarrow{G(g)} G(M) \xrightarrow{G(f)} G(M')$$

is also exact.

The functor G is *right exact* if, for every exact sequence

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M''$$

the induced sequence

$$G(M'') \xrightarrow{G(g)} G(M) \xrightarrow{G(f)} G(M') \to 0$$

is also exact.

THEOREM 7.2. *Let R be a ring and let N be an R-module. Then the functors $\mathrm{Hom}_R(N,-)\colon R\text{-}mod \to \mathcal{A}b$ and $\mathrm{Hom}_R(-,N)\colon R\text{-}mod \to \mathcal{A}b$ are left exact.*

PROOF. We will show that $\mathrm{Hom}_R(N,-)$ is left exact. The verification for $\mathrm{Hom}_R(-,N)$ is similar.

Consider an exact sequence

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M''.$$

We need to show that the induced sequence

$$0 \to \mathrm{Hom}_R(N,M') \xrightarrow{\mathrm{Hom}_R(N,f)} \mathrm{Hom}_R(N,M) \xrightarrow{\mathrm{Hom}_R(N,g)} \mathrm{Hom}_R(N,M'')$$

is exact.

1. $\mathrm{Hom}_R(N,f)$ is 1-1. Let $\phi \in \mathrm{Ker}(\mathrm{Hom}_R(N,f)) \subseteq \mathrm{Hom}_R(N,M')$. Then $0 = \mathrm{Hom}_R(N,f)(\phi) = f \circ \phi$. Since f is 1-1, it follows that $\phi = 0$.

2. $\mathrm{Ker}(\mathrm{Hom}_R(N,g)) \supseteq \mathrm{Im}(\mathrm{Hom}_R(N,f))$. The fact that $\mathrm{Hom}_R(N,-)$ is a functor provides the first equality in the following sequence

$$\mathrm{Hom}_R(N,g) \circ \mathrm{Hom}_R(N,f) = \mathrm{Hom}_R(N, g \circ f) = \mathrm{Hom}_R(N,0) = 0.$$

The second equality follows from the exactness of the original sequence. The third equality is straightforward.

3. $\mathrm{Ker}(\mathrm{Hom}_R(N,g)) \subseteq \mathrm{Im}(\mathrm{Hom}_R(N,f))$. Let $\phi \in \mathrm{Ker}(\mathrm{Hom}_R(N,g)) \subseteq \mathrm{Hom}_R(N,M)$. Then $0 = \mathrm{Hom}_R(N,g)(\phi) = g \circ \phi$ and it follows that $\mathrm{Im}(\phi) \subseteq \mathrm{Ker}(g) = \mathrm{Im}(f)$. For every $n \in N$, this implies that $\phi(n) = f(m'_n)$ for some $m'_n \in M'$. Furthermore, since f is 1-1, the element m'_n is the unique element $m' \in M'$ such that $\phi(n) = f(m')$.

Define $\psi\colon N \to M'$ by the rule $\psi(n) = m'_n$. This is well-defined by the previous paragraph.

Claim: ψ is an R-module homomorpism. By definition, $m'_{n_1+n_2}$ is the unique element $m' \in M'$ such that $\phi(n_1+n_2) = f(m')$. By assumption, we have

$$f(m_{n_1} + m_{n_2}) = f(m_{n_1}) + f(m_{n_2}) = \phi(n_1) + \phi(n_2) = \phi(n_1+n_2).$$

Hence, the uniqueness of $m'_{n_1+n_2}$ implies that

$$\psi(n_1+n_2) = m'_{n_1+n_2} = m_{n_1} + m_{n_2} = \psi(n_1) + \psi(n_2).$$

A similar argument shows that $\psi(rn) = r\psi(n)$.

Thus, we have $\psi \in \mathrm{Hom}_R(N, M')$. Now we show that $\mathrm{Hom}_R(N,f)(\psi) = \phi$:

$$(\mathrm{Hom}_R(N,f)(\psi))(n) = f(\psi(n)) = f(m'_n) = \phi(n).$$

Hence, we have $\phi \in \mathrm{Im}(\mathrm{Hom}_R(N,f))$, and we are done. □

PROPOSITION 7.3. *Let R be a ring with identity. For each $n \geqslant 0$, the functor $\mathrm{Hom}_R(R^n, -)$ is exact.*

PROOF. It is straightforward to show (exercise) that the functor $(-)^n$ is exact. The isomorphism $\mathrm{Hom}_R(R^n,-) \cong (-)^n$ yields the desired result. □

8. Day 8

The functors $\mathrm{Hom}_R(N,-)$ and $\mathrm{Hom}_R(-,N)$ are not usually exact:

EXAMPLE 8.1. Consider the sequence of $\mathbb{Z}$-modules

$$(*) \qquad 0 \to \mathbb{Z} \xrightarrow{\mu_2} \mathbb{Z} \xrightarrow{\tau} \mathbb{Z}/(2) \to 0$$

where $\mu_2(n) = 2n$ and $\tau(m) = \overline{m}$. This sequence is exact. However, the sequences $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(2), *)$ and $\mathrm{Hom}_{\mathbb{Z}}(*, \mathbb{Z}/(2))$ are not exact, as follows.

To see that the sequence $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(2),*)$ is not exact, we need to show that the sequence

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(2),\mathbb{Z}) \xrightarrow{\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(2),\tau)} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(2),\mathbb{Z}/(2)) \to 0$$

is not exact, that is, that the map $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(2),\tau)$ is not onto. We show that $\mathrm{id}_{\mathbb{Z}/(2)} \colon \mathbb{Z}/(2) \to \mathbb{Z}/(2)$ is not in $\mathrm{Im}(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(2),\tau))$. By definition, it suffices to show that there does not exist a $\mathbb{Z}$-module homomorphism $\phi \colon \mathbb{Z}/(2) \to \mathbb{Z}$ making the following diagram commute.

$$\begin{array}{ccc} & & \mathbb{Z}/(2) \\ & \overset{\nexists \phi}{\swarrow} & \big\downarrow = \\ \mathbb{Z} & \xrightarrow{\tau} & \mathbb{Z}/(2). \end{array}$$

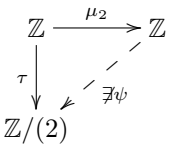
Note that the only $\mathbb{Z}$-module homomorphism $\phi \colon \mathbb{Z}/(2) \to \mathbb{Z}$ is the zero map $\phi = 0$, and this map does not make the diagram commute. (Another way to see this: The map ϕ would give a splitting of the sequence $(*)$, which would imply that $\mathbb{Z} \cong \mathbb{Z} \oplus \mathbb{Z}/(2)$, which is impossible.)

To see that the sequence $\mathrm{Hom}_{\mathbb{Z}}(*, \mathbb{Z}/(2))$ is not exact, we need to show that the sequence

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}/(2)) \xrightarrow{\mathrm{Hom}_{\mathbb{Z}}(\mu_2,\mathbb{Z}/(2))} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}/(2)) \to 0$$

is not exact, that is, that the map $\mathrm{Hom}_{\mathbb{Z}}(\mu_2,\mathbb{Z}/(2))$ is not onto. We show that $\tau \colon \mathbb{Z} \to \mathbb{Z}/(2)$ is not in $\mathrm{Im}(\mathrm{Hom}_{\mathbb{Z}}(\mu_2,\mathbb{Z}/(2)))$. By definition, it suffices to show

that there does not exist a $\mathbb{Z}$-module homomorphism $\psi\colon \mathbb{Z} \to \mathbb{Z}/(2)$ making the following diagram commute.



Let $\psi\colon \mathbb{Z}/(2) \to \mathbb{Z}$. Then $\psi(\mu_2(1)) = \psi(2) = 2\psi(1) = 0 \neq \tau(1)$, so ψ does not make the diagram commute.

PROPOSITION 8.2. *Let $F\colon R\text{-}mod \to \mathcal{A}b$ be a covariant additive functor. TFAE.*

(i) *The functor F is exact;*
(ii) *The functor F is left exact and right exact;*
(iii) *For every short exact sequence of R-module homomorphisms*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

the resulting sequence

$$0 \to F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'') \to 0$$

is exact.

PROOF. The implications (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii) follow from the definitions.
(iii) $\Longrightarrow$ (i). Assume that condition (iii) holds and consider an exact sequence

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3.$$

We need to show that the sequence

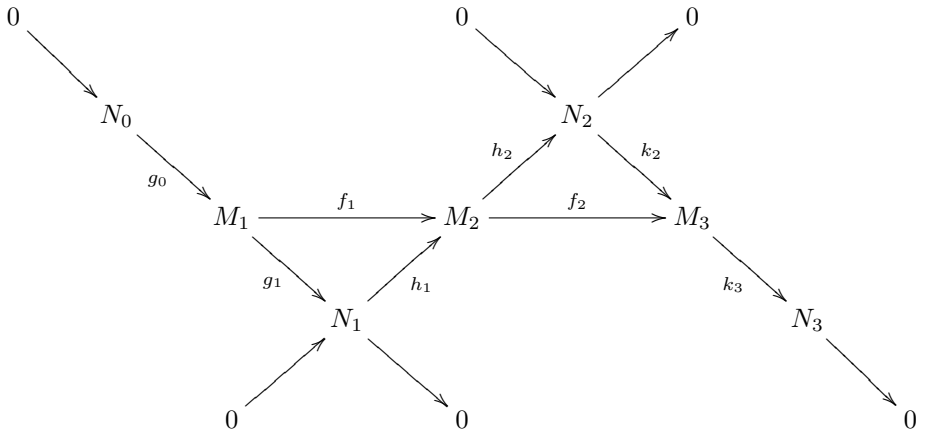
$$F(M_1) \xrightarrow{F(f_1)} F(M_2) \xrightarrow{F(f_2)} F(M_3)$$

is exact. Since F is an additive functor, we have

$$F(f_2) \circ F(f_1) = F(f_2 \circ f_1) = F(0) = 0.$$

Thus, we have $\mathrm{Im}(F(f_1)) \subseteq \mathrm{Ker}(F(f_2))$, and it remains to show that $\mathrm{Im}(F(f_1)) \supseteq \mathrm{Ker}(F(f_2))$.

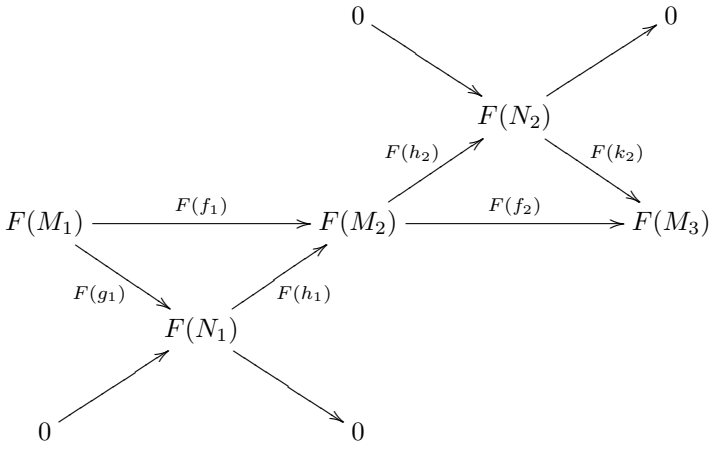
Consider the following commutative diagram



where

$$\begin{aligned} N_0 &= \operatorname{Ker}(f_1) & N_1 &= \operatorname{Im}(f_1) = \operatorname{Ker}(f_2) \\ N_2 &= \operatorname{Im}(f_2) & N_3 &= M_3/K_2 \\ g_0(n_0) &= n_0 & g_1(m_1) &= f_1(m_1) \\ h_1(n_1) &= n_1 & h_2(m_2) &= f_2(m_2) \\ k_2(n_2) &= n_2 & k_3(m_3) &= \overline{m_3} \end{aligned}$$

Note that the diagonal sequences of this diagram are short exact sequences by design. Thus, our assumption on F implies that the diagonal sequences of the following diagram are also exact



Also, this diagram commutes because F is a functor.

To show that $\operatorname{Im}(F(f_1)) \supseteq \operatorname{Ker}(F(f_2))$, let $x_2 \in \operatorname{Ker}(F(f_2))$. Then

$$0 = F(f_2)(x_2) = F(k_2)(F(h_2)(x_2))$$

and so the fact that $F(k_2)$ is 1-1 implies that $F(h_2)(x_2) = 0$. Hence, we have

$$x_2 \in \operatorname{Ker}(F(h_2)) = \operatorname{Im}(F(h_1))$$

so there exists $y_1 \in F(N_1)$ such that $F(h_1)(y_1) = x_2$. Since $F(g_1)$ is surjective, there exists $x_1 \in F(M_1)$ such that $y_1 = F(g_1)(x_1)$. Thus, we have

$$F(f_1)(x_1) = F(h_1)(F(g_1)(x_1)) = F(h_1)(y_1) = x_2 \in \operatorname{Im}(F(f_1))$$

as desired. □

PROPOSITION 8.3. *Let $G\colon R\text{-mod} \to \mathcal{A}b$ be a contravariant additive functor. TFAE.*

(i) *The functor G is exact;*
(ii) *The functor G is left exact and right exact;*
(iii) *For every short exact sequence of R-module homomorphisms*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

the resulting sequence

$$0 \to G(M') \xrightarrow{G(f)} G(M) \xrightarrow{G(g)} G(M'') \to 0$$

is exact.

PROOF. Similar to Proposition 8.2. □

DEFINITION 8.4. Let R be a ring. An R-module P is *projective* if the functor $\mathrm{Hom}_R(P, -)$ is exact.

REMARK 8.5. The functor $\mathrm{Hom}_R(M, -)$ is always left exact. Thus, Proposition 8.2 implies that P is projective if and only if, for every R-module epimorphism $f\colon M \twoheadrightarrow M''$ the induced map $\mathrm{Hom}_R(P, f)\colon \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, M'')$ is surjective.

Proposition 7.3 says that, when R has identity, the module R^n is projective. The next result generalizes this.

PROPOSITION 8.6. *Let R be a ring with identity, and let F be a free R-module. Then F is projective.*

PROOF. It suffices to consider an exact sequence

$$M \xrightarrow{g} M'' \to 0$$

and show that the resulting sequence

$$\mathrm{Hom}_R(F, M) \xrightarrow{\mathrm{Hom}_R(F,g)} \mathrm{Hom}_R(F, M'') \to 0$$

is exact. Fix an R-module homomorphism $f \in \mathrm{Hom}_R(F, M'')$ and consider the diagram

$$\begin{array}{ccccc} & & & & F \\ & & \swarrow^{\exists h} & & \downarrow f \\ M & \xrightarrow{g} & M'' & \longrightarrow & 0. \end{array}$$

It suffices to find h making the diagram commute.

Let $B \subseteq F$ be a basis for F as an R-module. The map g is surjective. For each $b \in B$, choose an element $m_b \in M$ such that $g(m_b) = f(b)$. Define $h\colon F \to M$ by the formula $h(\sum_{b\in B} r_b b) = \sum_{b\in B} r_b m_b$. Proposition 4.2.4 shows that h is a well-defined R-module homomorphism. Also, we have

$$g(h(\textstyle\sum_{b\in B} r_b b)) = g(\sum_{b\in B} r_b m_b) = \sum_{b\in B} r_b g(m_b) = \sum_{b\in B} r_b f(b) = f(\sum_{b\in B} r_b b)$$

and so

$$f = gh = \mathrm{Hom}_R(F, g)(h).$$

It follows that $\mathrm{Hom}_R(F, g)$ is surjective, as desired. □

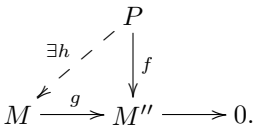
The implication (iv) $\Longrightarrow$ (i) in the next result generalizes the previous result.

PROPOSITION 8.7. *Let R be a ring with identity, and let P be a unitary R-module. TFAE.*

(i) *P is a projective R-module;*
(ii) *For every diagram of unitary R-module homomorphisms with exact bottom row*

$$\begin{array}{ccccc} & & & & P \\ & & & & \downarrow f \\ M & \xrightarrow{g} & M'' & \longrightarrow & 0 \end{array}$$

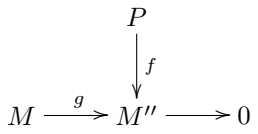
there is an R-module homomorphism $h\colon P \to M$ making the next diagram commute



(iii) *Every exact sequence of the form $0 \to M' \to M \to P \to 0$ splits;*
(iv) *There is a unitary R-module M' such that $P \oplus M'$ is free.*

REMARK 8.8. Note that the map h in condition (ii) need not be unique.

PROOF. (i) $\implies$ (ii). Assume that P is projective and consider a diagram



with exact bottom row. The functor $\mathrm{Hom}_R(P, -)$ is exact, so we have an exact sequence

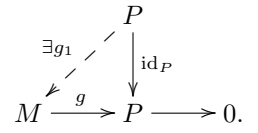
$$\mathrm{Hom}_R(P, M) \xrightarrow{\mathrm{Hom}_R(P,g)} \mathrm{Hom}_R(P, M'') \to 0.$$

The given map f is in $\mathrm{Hom}_R(P, M'')$, so there exists $h \in \mathrm{Hom}_R(P, M)$ such that

$$f = \mathrm{Hom}_R(P, g)(h) = g \circ h.$$

Hence h makes the desired diagram commute.

(ii) $\implies$ (iii). Assume condition (ii) holds and consider an exact sequence $0 \to M' \to M \to P \to 0$. This gives a commutative diagram



The map h satisfies $gg_1 = \mathrm{id}_P$, so the sequence splits by Proposition 3.3.

(iii) $\implies$ (iv). Proposition 4.4.1(a) a free R-module F and a surjection $\tau\colon F \to M$. Condition (iii) implies that the exact sequence

$$0 \to \mathrm{Ker}(\tau) \to F \xrightarrow{\tau} P \to 0$$

splits, and so $F \cong \mathrm{Ker}(\tau) \oplus P$.

(iv) $\implies$ (i). Write $F = P \oplus M'$. Proposition 8.6 shows that F is projective. By an exercise, we know that

$$\mathrm{Hom}_R(F, -) \cong \mathrm{Hom}_R(P \oplus M', -) \cong \mathrm{Hom}_R(P, -) \oplus \mathrm{Hom}_R(M', -).$$

This functor is exact, so another exercise implies that the functors $\mathrm{Hom}_R(P, -)$ and $\mathrm{Hom}_R(M', -)$ are exact. Thus P is projective. □

9. Day 9

Here is an example of a ring with a non-free projective module.

EXAMPLE 9.1. Let R_1 and R_2 be rings with identity and set $R = R_1 \times R_2$. The modules $P_1 = R_1 \times 0$ and $P_2 = 0 \times R_2$ are both projective because $P_1 \oplus P_2 \cong R$. Note that P_1 is not free because the element $(0,1) \in R$ is nonzero and $(0,1)P_1 = 0$.

DEFINITION 9.2. Let R be a ring. An R-module I is *injective* if the functor $\mathrm{Hom}_R(-, I)$ is exact.

REMARK 9.3. The functor $\mathrm{Hom}_R(-, N)$ is always left exact. Thus, Proposition 8.2 implies that I is injective if and only if, for every R-module monomorphism $f\colon M' \hookrightarrow M$ the induced map $\mathrm{Hom}_R(f, I)\colon \mathrm{Hom}_R(M, I) \to \mathrm{Hom}_R(M', I)$ is surjective.

PROPOSITION 9.4. *Let R be a ring with identity, and let I be a unitary R-module. TFAE.*

(i) *I is an injective R-module;*
(ii) *For every diagram of unitary R-module homomorphisms with exact top row*

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M \\ & & \downarrow{\scriptstyle g} & & \\ & & I & & \end{array}$$

there is an R-module homomorphism $h\colon M \to I$ making the next diagram commute

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M \\ & & \downarrow{\scriptstyle g} & \swarrow{\scriptstyle \exists h} & \\ & & I. & & \end{array}$$

□

REMARK 9.5. Note that the map h in condition (ii) need not be unique.

Also, note the absence of a condition corresponding to Proposition 8.7(iii) and (iv). We will prove the analogue of (iii) below. There is no version of (iv).

Examples of injective modules are more difficult to construct. We will see (exercise) that $\mathbb{Q}$ is an injective $\mathbb{Z}$-module. This can be proved using the next result. See also Lemma 10.4.

THEOREM 9.6 (Baer's Criterion). *Let R be a ring with identity and J a unitary R-module. TFAE:*

(i) *J is an injective R-module;*
(ii) *For every ideal $I \subseteq R$ and every R-module homomorphism $g\colon I \to J$, there exists an R-module homomorphism $h\colon R \to J$ making the following diagram commute*

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{\subseteq} & R \\ & & \downarrow{\scriptstyle g} & \swarrow{\scriptstyle \exists h} & \\ & & J. & & \end{array}$$

PROOF. (i) $\implies$ (ii). By Proposition 9.4.

(ii) $\implies$ (i). Consider a diagram of unitary R-module homomorphisms with exact top row

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M \\ & & {\scriptstyle g}\downarrow & \swarrow_{\exists h} & \\ & & I. & & \end{array}$$

We need to find an R-module homomorphism $h\colon M \to I$ making the diagram commute. for this, we use Zorn's Lemma. Set

$$S = \{R\text{-module homomorphisms } h\colon C \to J \mid \mathrm{Im}(f) \subseteq C \subseteq M \text{ and } hf = g\}.$$

Partially order S as follows: $(h_1\colon C_1 \to J) \leqslant (h_2\colon C_2 \to J)$ if and only if $C_1 \subseteq C_2$ and $h_2|_{C_1} = h_1$. Check that this is a partial order on S.

Claim: S satisfies the hypotheses of Zorn's Lemma. Let $\mathcal{C}$ be a nonempty chain in S. Define $D = \cup_{(h\colon C \to J) \in \mathcal{C}} C$. Since $\mathcal{C}$ is a chain in S, it follows that D is a submodule of M such that $\mathrm{Im}(f) \subseteq D$. Define $k\colon D \to J$ as follows. For each $d \in D$, there exists $(h\colon C \to J) \in \mathcal{C}$ such that $d \in C$; set $k(d) = h(d)$. Since $\mathcal{C}$ is a chain, it follows that $k(d)$ is independent of the choice of $(h\colon C \to J) \in \mathcal{C}$. Since $\mathcal{C}$ is a chain and each $(h\colon C \to J) \in \mathcal{C}$ is an R-module homomorphism, it is straightforward to show that k is an R-module homomorphism and that $kf = g$. In other words, $k\colon D \to J$ is in S. By construction, $(h\colon C \to J) \leqslant (k\colon D \to J)$ for each $(h\colon C \to J) \in \mathcal{C}$, and so $(k\colon D \to J)$ is an upper bound for $\mathcal{C}$ in S.

Zorn's Lemma implies that S has a maximal element $(h\colon C \to J)$. We will use the maximality to show that $C = M$. It will then follow that $(h\colon M \to J) \in S$, and so $h\colon M \to J$ makes the desired diagram commute.

Suppose that $C \subsetneq M$ and let $m \in M \smallsetminus C$. Set

$$I = \{r \in R \mid rm \in C\}.$$

Check that this is a left ideal of R. Define $\phi\colon I \to J$ by the formula $\phi(r) = h(rm)$. Check that this is an R-module homomorphism. Condition (ii) yields an R-module homomorphism $\psi\colon R \to J$ making the following diagram commute

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{\subseteq} & R \\ & & {\scriptstyle \phi}\downarrow & \swarrow_{\psi} & \\ & & J. & & \end{array}$$

Define $C' = C + Rm$ which is a submodule of M such that $\mathrm{Im}(g) \subseteq C \subsetneq C' \subseteq M$. We will construct an R-module homomorphism $h'\colon C' \to J$ such that $h'f = g$ and $h'|_C = h$; this will show that $(h'\colon C' \to J) \in S$ and $(h\colon C \to J) < (h'\colon C' \to J)$, thus contradicting the maximality of $(h\colon M \to J)$ in S.

Define $h'\colon C' \to J$ by the formula $h'(c + rm) = h(c) + \psi(r)$. We need to show that this is well-defined, so suppose that $c + rm = c_1 + r_1 m$. It follows that $(r - r_1)m = rm - r_1 m = c_1 - c \in C$, and so $r - r_1 \in I$.

$$h(c_1) - h(c) = h(c_1 - c) = h((r - r_1)m) = \phi(r - r_1) = \psi(r - r_1) = \psi(r) - \psi(r_1)$$

and so $h(c_1) + \psi(r_1) = h(c) + \psi(r)$. Thus, h' is well-defined.

It is straightforward to show that h' is an R-module homomorphism, because h and ψ are R-module homomorphisms. For $m' \in M'$ we have $f(m') \in \mathrm{Im}(f) \subseteq C$ and so (using $c = f(m')$ and $r = 0$) we have

$$h'(f(m')) = h(f(m')) = g(m')$$

because $hf = g$. It follows that $h'f = g$ as well. A similar argument shows that $h'|_C = h$, as desired. □

REMARK 9.7. The notion of "injective" is in a sense dual to the notion of "projective". For projective modules, we know the following: Every unitary module over a ring with identity is a homomorphic image of a projective R-module. The "dual" result says that every unitary module over a ring with identity is a submodule of an injective R-module. This result takes more work to prove. We begin with the case $R = \mathbb{Z}$.

10. Day 10

DEFINITION 10.1. An abelian group D is *divisible* if, for each $d \in D$ and for each $0 \neq n \in \mathbb{Z}$, there exists $e \in D$ such that $ne = d$.

REMARK 10.2. These groups are "divisible" because you can always solve the division problem $d \div n$ in D.

EXAMPLE 10.3. $\mathbb{Q}$ is a divisible abelian group.

LEMMA 10.4. *An abelian group G is divisible if and only if it is injective as a unitary $\mathbb{Z}$-module.*

PROOF. $\Longrightarrow$: Assume that G is divisible. We use Baer's criterion. Let $I \subseteq \mathbb{Z}$ be an ideal and let $g\colon I \to G$ be a $\mathbb{Z}$-module homomorphism. Then $I = n\mathbb{Z}$ for some $n \geqslant 0$. We need to find a $\mathbb{Z}$-module homomorphism $h\colon \mathbb{Z} \to G$ making the following diagram commute

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{\subseteq} & \mathbb{Z} \\ & & {\scriptstyle g}\downarrow & \swarrow_{\exists h} & \\ & & G. & & \end{array}$$

The case $n = 0$ is straightforward using $h = 0$, so assume that $n > 0$. Since G is divisible, there exists $a \in G$ such that $na = g(n)$. It follows that $g(mn) = mg(n) = mna$ for all $m \in \mathbb{Z}$. Define $h\colon \mathbb{Z} \to G$ as $h(m) = ma$ for all $m \in \mathbb{Z}$. This is a well-defined $\mathbb{Z}$-module homomorphism such that $h|_I = g$, as desired.

$\Longleftarrow$: Assume that G is injective. To show that G is divisible, let $0 \neq n \in \mathbb{Z}$ and let $b \in G$. We need to find an element $c \in G$ such that $nc = b$. Define $g\colon n\mathbb{Z} \to G$ by the formula $g(nm) = mb$. This is a well-defined $\mathbb{Z}$-module homomorphism, so the fact that G is injective provides a $\mathbb{Z}$-module homomorphism $h\colon \mathbb{Z} \to G$ making the following diagram commute

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{\subseteq} & \mathbb{Z} \\ & & {\scriptstyle g}\downarrow & \swarrow_{\exists h} & \\ & & G. & & \end{array}$$

In particular, the element $c = h(1)$ satisfies

$$nc = nh(1) = h(n) = b$$

as desired. □

LEMMA 10.5. *Let G be an abelian group. Then there is a divisible abelian group D and an abelian group monomorphism $f\colon G \hookrightarrow D$.*

PROOF. Let $\tau\colon F \to G$ be an epimorphism such that F is a free abelian group. Let $K = \mathrm{Ker}(\tau)$ so that we have $G \cong F/K$. Write $F \cong \mathbb{Z}^{(\Lambda)}$ for some set Λ and set $D_1 = \mathbb{Q}^{(\Lambda)}$. An exercise shows that D is divisible. It is straightforward to construct an abelian group monomorphism $i\colon \mathbb{Z}^{(\Lambda)} \hookrightarrow \mathbb{Q}^{(\Lambda)}$, i.e., $i\colon F \hookrightarrow D_1$. Since i is a monomorphism, it follows that

$$G \cong F/K \cong i(F)/i(K) \subseteq D_1/i(K).$$

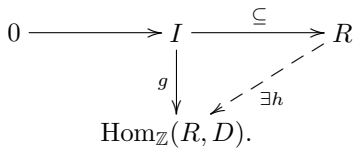
(Exercise. Use Proposition 6.2.) Since D_1 is divisible, so is the quotient $D_1/i(K)$, and so we have the desired monomorphism. □

Here is a way to construct injective R-modules.

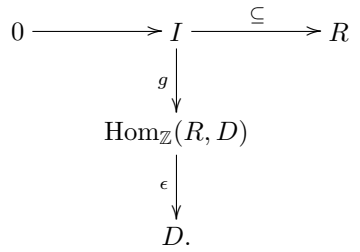
LEMMA 10.6. *Let R be a ring with identity. If D is a divisible abelian group, then $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is an injective R-module.*

PROOF. First, observe that R is an additive abelian group, hence R is a unitary $\mathbb{Z}$-module. Thus $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ makes sense. Next, we define an R-module structure on $\mathrm{Hom}_{\mathbb{Z}}(R, D)$: for $r \in R$ and $\phi \in \mathrm{Hom}_{\mathbb{Z}}(R, D)$, define $r\phi\colon R \to D$ as $(r\phi)(s) = \phi(sr)$. Check that $r\phi$ is a $\mathbb{Z}$-module homomorphism, and that this make $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ into an R-module.

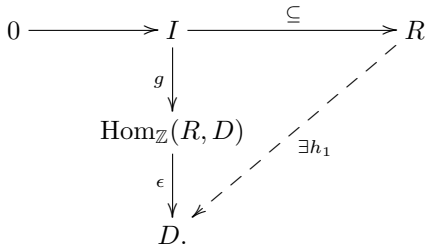
We now use Baer's Criterion to show that $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is an injective R-module. Let $I \subseteq R$ be an ideal, and let $g\colon I \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$ be an R-module homomorphism. We need to show that there exists an R-module homomorphism $h\colon R \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$ making the following diagram commute



The evaluation map $\epsilon\colon \mathrm{Hom}_{\mathbb{Z}}(R, D) \to D$ given by $\epsilon(\phi) = \phi(1)$ is an abelian group homomorphism, so we have a diagram of abelian group homomorphisms



Since D is divisible, it is injective as a $\mathbb{Z}$-module, so there exists an abelian group homomorphism $h_1 \colon R \to D$ making the next diagram commute:



Define $h \colon R \to \mathrm{Hom}_\mathbb{Z}(R, D)$ as follows. For $r \in R$, we let $h(r) \colon R \to D$ by the formula $h(r)(s) = h_1(sr)$. Check that $h(r) \in \mathrm{Hom}_\mathbb{Z}(R, D)$, which shows that h is a well-defined function. [You need to show that $h(r)$ is an abelian group homomorphism, that is, that $h(r)(s + s') = h(r)(s) + h(r)(s')$ for all $r, s, s' \in R$.] Check that h is an abelian group homomorphism. [You need to show that $h(r+r') = h(r) + h(r')$, that is, that $h(r + r')(s) = h(r)(s) + h(r')(s)$ for all $r, r', s \in R$.]

Claim: h is an R-module homomorphism. We need to show that $h(rr') = rh(r')$ for all $rr' \in R$, that is, that $[h(rr')](s) = [rh(r')](s)$ for all $rr' \in R$.

$$[h(rr')](s) = h_1(s(rr')) = h_1((sr)r') = h(r')(sr) = [rh(r')](s)$$

Claim: for all $a \in I$, we have $h(a) = g(a)$. (Once this is shown, we will have shown that the desired diagram commutes, and we'll be done.) We need to show that $h(a)(r) = g(a)(r)$ for all $r \in R$. Note that, since $a \in I$ and $r \in R$, we have $ra \in I$.

$$h(a)(r) = h_1(ra) = \epsilon(g(ra)) = g(ra)(1) = [rg(a)](1) = g(a)(1 \cdot r) = g(a)(r)$$

as desired. □

THEOREM 10.7. *Let R be a ring with identity and let M be a unitary R-module. Then there exists an R-module monomorphism $M \hookrightarrow J$ where J is an injective unitary R-module.*

PROOF. M is an additive abelian group, so Lemma 10.5 yields an abelian group monomorphism $f \colon M \hookrightarrow D$ where D is a divisible abelian group. The induced map $\mathrm{Hom}_\mathbb{Z}(R, f) \colon \mathrm{Hom}_\mathbb{Z}(R, M) \to \mathrm{Hom}_\mathbb{Z}(R, D)$ is an abelian group homomorphism. It is a monomorphism because $\mathrm{Hom}_\mathbb{Z}(R, -)$ is left exact. Check that it is an R-module homomorphism. This yields a sequence

$$M \xrightarrow{\cong} \mathrm{Hom}_R(R, M) \subseteq \mathrm{Hom}_\mathbb{Z}(R, M) \hookrightarrow \mathrm{Hom}_\mathbb{Z}(R, D)$$

where the inclusion comes from the fact that every R-module homomorphism $R \to M$ is, in particular, an abelian group homomorphism. The composition of these maps is an R-module monomorphism. The R-module $J = \mathrm{Hom}_\mathbb{Z}(R, D)$ is injective by Lemma 10.6, giving the desired result. □

Here is the version of Proposition 8.7 for injectives.

PROPOSITION 10.8. *Let R be a ring with identity, and let I be a unitary R-module. TFAE.*

(i) *I is an injective R-module;*
(ii) *Every exact sequence of the form $0 \to I \to M \to M'' \to 0$ splits.*

PROOF. (i) $\implies$ (ii) Assume that I is injective and consider an exact sequence $0 \to I \xrightarrow{f} M \to M'' \to 0$. Proposition 9.4 yields an R-module homomorphism $f_1 \colon M \to I$ making the next diagram commute

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{f} & M \\ & & \downarrow{\scriptstyle \mathrm{id}_I} & \swarrow{\scriptstyle \exists f_1} & \\ & & I & & \end{array}$$

so the sequence splits.

(ii) $\implies$ (i) Theorem 10.7 shows that there is an R-module monomorphism $f \colon I \to J$ such that J is injective. Condition (ii) implies that the resulting short exact sequence splits

$$0 \to I \xrightarrow{f} J \to J/I \to 0$$

and so $J \cong I \oplus J/I$. The fact that J is injective implies that I and J/I are injective (exercise) as desired. □

11. Day 11

Now for tensor products.

REMARK 11.1. Let R be a ring. The function $\mu \colon R \times R$ given by $\mu(r, s) = rs$ is not as well-behaved as one might like. For instance, it is not an R-module homomorphism:

$$\mu((1,0) + (0,1)) = \mu(1,1) = 1 \neq 0 = \mu(1,0) + \mu(0,1).$$

In a sense, the tensor product fixes this problem.

DEFINITION 11.2. Let R be a ring. Let M be a right R-module and let N be a left R-module. Let G be an abelian group. A function $f \colon M \times N \to G$ is *R-biadditive* if

$$\begin{aligned} f(m + m', n) &= f(m, n) + f(m', n) \\ f(m, n + n') &= f(m, n) + f(m, n') \\ f(mr, n) &= f(m, rn) \end{aligned}$$

for all $m, m' \in M$ all $n, n' \in N$ and all $r \in R$.

EXAMPLE 11.3. Let R be a ring. The function $\mu \colon R \times R$ given by $\mu(r, s) = rs$ is the prototype of an R-biadditive function.

DEFINITION 11.4. Let R be a ring. Let M be a right R-module and let N be a left R-module. A *tensor product* of M and N over R is an abelian group $M \otimes_R N$ equipped with an R-biadditive function $h \colon M \times N \to M \otimes_R N$ satisfying the following universal property: For every abelian group G and every R-biadditive function $f \colon M \times N \to G$, there exists a unique abelian group homomorphism $F \colon M \otimes_R N \to G$ making the following diagram commute

$$\begin{array}{ccc} M \times N & \xrightarrow{h} & M \otimes_R N \\ & \searrow^{f} & \downarrow{\scriptstyle \exists! F} \\ & & G. \end{array}$$

THEOREM 11.5. *Let R be a ring. Let M be a right R-module and let N be a left R-module. Then $M \otimes_R N$ exists.*

PROOF. Existence. Consider $\mathbb{Z}^{(M\times N)}$, the free abelian group with basis $M\times N$. For $m \in M$ and $n \in N$, let $(m,n) \in \mathbb{Z}^{(M\times N)}$ denote the corresponding basis vector. Let $\epsilon\colon M \times N \to \mathbb{Z}^{(M\times N)}$ be the function $\epsilon(m,n) = (m,n)$. Set

$$H = \left\langle \begin{array}{c} (m+m',n)-(m,n)-(m',n) \\ (m,n+n')-(m,n)-(m,n') \\ (mr,n)-(m,rn) \end{array} \middle| \begin{array}{c} m,m' \in M \\ n,n' \in N \\ r \in R \end{array} \right\rangle \subseteq \mathbb{Z}^{(M\times N)}.$$

Set $M \otimes_R N = \mathbb{Z}^{(M\times N)}/H$ and, for $m \in M$ and $n \in N$ write

$$m \otimes n = [(m,n)] = (m,n) + H \in \mathbb{Z}^{(M\times N)}/H = M \otimes_R N.$$

Define $h\colon M \times N \to M \otimes_R N$ to be the composition

$$M \times N \xrightarrow{\varepsilon} \mathbb{Z}^{(M\times N)} \xrightarrow{\pi} \mathbb{Z}^{(M\times N)}/H = M \otimes_R N$$

that is, by the rule $h(m,n) = m \otimes n$.

It is straightforward to show that h is well-defined and R-biadditive. For example, we have

$$\begin{aligned} h(m+m',n) &= (m+m') \otimes n \\ &= [(m+m',n)] \\ &= [(m,n)] + [(m',n)] \\ &= m \otimes n + m' \otimes n \\ &= h(m,n) + h(m',n). \end{aligned}$$

In terms of tensors, the R-biadditivity of h reads as

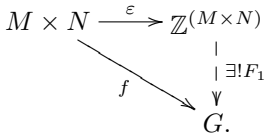
$$\begin{aligned} (m+m') \otimes n &= m \otimes n + m' \otimes n \\ m \otimes (n+n') &= m \otimes n + m \otimes n' \\ (mr) \otimes n &= m \otimes (rn) \end{aligned}$$

Note also that elements of $M \otimes_R N$ are of the form

$$[\textstyle\sum_i l_i(m_i,n_i)] = \sum_i l_i[(m_i,n_i)] = \sum_i l_i(m_i \otimes n_i).$$

We'll see later that, usually, there are elements of $M \otimes_R N$ that cannot be written as "simple tensors", that is, are not of the form $m \otimes n$.

To see that $M \otimes_R N$ satisfies the desired universal property, let G be an abelian group and $f\colon M \times N \to G$ an R-biadditive function. Use the universal property for free abelian groups Corollary 1.19.1 to see that there is a unique abelian group homomorphism $F_1\colon \mathbb{Z}^{(M\times N)} \to G$ such that $F_1(m,n) = f(m,n)$.

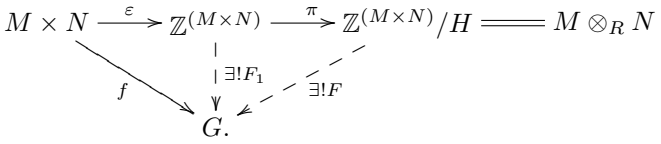


From the proof of Corollary 1.19.1, we have

$$F_1(\textstyle\sum_i l_i(m_i,n_i)) = \sum_i l_i f(m_i,n_i)).$$

Use this formula to check that each generator of H is in $\mathrm{Ker}(F_1)$; this will use the R-biadditivity of f. It follows that $H \subseteq \mathrm{Ker}(F_1)$ and so the universal property

for quotients Lemma 1.9.2 implies that there exists a unique abelian group homomorphism $F\colon \mathbb{Z}^{(M\times N)}/H \to G$ making the right-hand triangle in the next diagram commute



Thus, we see that the desired homomorphism F exists and is unique.

The above construction shows that F is given by the formula

$$F(\textstyle\sum_i l_i(m_i \otimes n_i)) = F([\sum_i l_i(m_i, n_i)]) = F_1(\sum_i l_i(m_i, n_i)) = \sum_i l_i f(m_i, n_i)).$$

□

EXAMPLE 11.6. Let R be a ring. Let M be a right R-module and let N be a left R-module. The computations in the proof of Theorem 11.5 show

$$(\textstyle\sum_i m_i r_i) \otimes n = \sum_i (m_i r_i) \otimes n = \sum_i m_i \otimes (r_i n)$$

for all $m_i \in M$, all $r_i \in R$ and all $n \in N$. Other formulas hold similarly. In particular, for $l_i \in \mathbb{Z}$, we have

$$\textstyle\sum_i l_i(m_i \otimes n_i) = \sum_i ((l_i m_i) \otimes n_i) = \sum_i m_i' \otimes n_i$$

where $m_i' = l_i m_i$.

The additive identity in $M \otimes_R N$ is $0_{M\otimes N} = 0_M \otimes 0_N$. This can be written several (seemingly) different ways. For instance, for each $n \in N$, we have

$$0_M \otimes n = (0_M 0_R) \otimes n = 0_M \otimes (0_R n) = 0_M \otimes 0_N.$$

Similarly, for all $m \in M$, we have $m \otimes 0_N = 0_M \otimes 0_N$.

REMARK 11.7. Let R be a ring. Let M be a right R-module and let N be a left R-module. It should be reiterated that there are more elements in $M \otimes_R N$ than the simple tensors $m \otimes n$. General elements of $M \otimes_R N$ are of the form $\sum_i m_i \otimes n_i$, as was shown in Example 11.6. However, certain properties of $M \otimes_R N$ are determined by their restrictions to the simple tensors, as we see in Lemma 11.8.

LEMMA 11.8. *Let R be a ring. Let M be a right R-module and let N be a left R-module. Let $\gamma, \delta\colon M \otimes_R N \to G$ be a abelian group homomorphisms.*

(a) *$M \otimes_R N = 0$ if and only if $m \otimes n = 0$ for all $m \in M$ and all $n \in N$.*
(b) *$\gamma = \delta$ if and only if $\gamma(m \otimes n) = \delta(m \otimes n)$ for all $m \in M$ and all $n \in N$.*
(c) *If $G = M \otimes_R N$, then $\gamma = \mathrm{id}_{M\otimes_R N}$ if and only if $\gamma(m \otimes n) = m \otimes n$ for all $m \in M$ and all $n \in N$.*
(d) *$\gamma = 0$ if and only if $\gamma(m \otimes n) = 0$ for all $m \in M$ and all $n \in N$.*

PROOF. Part (a) follows from the fact that every element of $M \otimes_R N$ is of the form $\sum_i m_i \otimes n_i = \sum_i 0 = 0$.

Part (b) can be proved similarly, or by using the uniqueness statement in the universal property.

Part (c) can be proved similarly, or by using the uniqueness statement in the universal property, or as the special case $\delta = \mathrm{id}_{M\otimes_R N}$ of part (b).

Part (d) can be proved similarly, or by using the uniqueness statement in the universal property, or as the special case $\delta = 0$ of part (b). □

12. Day 12

When proving properties about tensor products, we very rarely use the construction. Usually, we use the universal property, as in the following result.

THEOREM 12.1. *Let R be a ring. Let M be a right R-module and let N be a left R-module. Then $M \otimes_R N$ is unique up to abelian group isomorphism.*

PROOF. Assume that $h\colon M \times N \to M \otimes_R N$ and $k\colon M \times N \to M \odot_R N$ both satisfy the defining property for the tensor product, that is: $M \otimes_R N$ and $M \odot_R N$ are abelian groups, the functions h and k are R-biadditive, and for every abelian group G and every R-biadditive function $f\colon M \times N \to G$, there exists a unique abelian group homomorphism $F\colon M \otimes_R N \to G$ and $H\colon M \odot_R N \to G$ making the following diagrams commute

$$\begin{array}{ccc} M \times N & \xrightarrow{h} & M \otimes_R N \\ & \searrow^{f} & \downarrow{\scriptstyle \exists! F} \\ & & G \end{array} \qquad \begin{array}{ccc} M \times N & \xrightarrow{k} & M \odot_R N \\ & \searrow^{f} & \downarrow{\scriptstyle \exists! H} \\ & & G. \end{array}$$

Apply the universal property for $M \otimes_R N$ to the map $k\colon M \times N \to M \odot_R N$ to find an abelian group homomorphism $\phi\colon M \otimes N \to M \odot_R N$ making the following diagram commute

$$\begin{array}{ccc} M \times N & \xrightarrow{h} & M \otimes_R N \\ & \searrow^{k} & \downarrow{\scriptstyle \exists! \phi} \\ & & M \odot_R N. \end{array}$$

Apply the universal property for $M \odot_R N$ to the map $h\colon M \times N \to M \otimes_R N$ to find an abelian group homomorphism $\psi\colon M \otimes N \to M \odot_R N$ making the following diagram commute

$$\begin{array}{ccc} M \times N & \xrightarrow{k} & M \odot_R N \\ & \searrow^{h} & \downarrow{\scriptstyle \exists! \psi} \\ & & M \otimes_R N. \end{array}$$

It follows that the next diagrams commute

$$\begin{array}{ccc} M \times N & \xrightarrow{h} & M \otimes_R N \\ & \searrow^{h} & \downarrow{\scriptstyle \psi\phi} \\ & & M \otimes_R N \end{array} \qquad \begin{array}{ccc} M \times N & \xrightarrow{h} & M \otimes_R N \\ & \searrow^{h} & \downarrow{\scriptstyle \mathrm{id}_{M \otimes_R N}} \\ & & M \otimes_R N. \end{array}$$

Hence, the uniqueness statement in the universal property implies that $\psi\phi = \mathrm{id}_{M \otimes_R N}$. A similar argument shows that $\phi\psi = \mathrm{id}_{M \odot_R N}$ and so ϕ and ψ are inverse isomorphisms, as desired. □

PROPOSITION 12.2. *Let R be a ring with identity. Let M be a unital right R-module and let N be a unital left R-module. There are abelian group isomorphisms*

$$F\colon M \otimes_R R \xrightarrow{\cong} M \qquad \text{and} \qquad G\colon R \otimes_R N \xrightarrow{\cong} N$$

such that $F(m \otimes r) = mr$ and $G(r \otimes n) = rn$. In particular, we have $M \otimes_R R \cong M$ and $R \otimes_R N \cong N$ and $R \otimes_R R \cong R$.

PROOF. We will verify the claim for $M \otimes_R R$. The map $f\colon M \times R \to M$ given by $f(m,r) = mr$ is R-biadditive. Hence, the universal property yields a unique R-module homomorphism $F\colon M \otimes_R R \to M$ such that $F(m \otimes r) = mr$ for all $m \in M$ and $r \in R$. We will show that F is bijective. The main point is the following computation in $M \otimes_R R$

$$\textstyle\sum_i (m_i \otimes r_i) = \sum_i ((m_i r_i) \otimes 1) = (\sum_i m_i r_i) \otimes 1$$

which shows that every element of $M \otimes_R R$ is of the form $m \otimes 1$.

F is surjective: $m = F(m \otimes 1)$.

F is injective: $0 = F(m \otimes 1)$ implies $0 = F(m \otimes 1) = m \cdot 1 = m$ implies $0 = 0 \otimes 1 = m \otimes 1$. □

REMARK 12.3. Note that we have not shown that the isomorphisms in Proposition 12.2 are R-module isomorphisms. This is because we have not shown, for instance, that $M \otimes_R R$ has an R-module structure. However, because R is also a right R-module (technically, it is an "RR-bimodule") it follows that $M \otimes_R R$ has a right R-module structure given by $(m \otimes r)r' = m \otimes (rr')$. Furthermore, this structure makes the isomorphism F into a homomorphism of right R-modules.

We will address this in the case when R is commutative below.

REMARK 12.4. It should be noted that other tensor products of R with itself, like $R \otimes_{\mathbb{Z}} R$ are not usually so simple. In fact, even when R is noetherian, the ring $R \otimes_{\mathbb{Z}} R$ is often not noetherian.

Here is the functoriality of tensor product.

PROPOSITION 12.5. *Let R be a ring. Let $\alpha\colon M \to M'$ and $\alpha'\colon M' \to M''$ be homomorphisms of right R-modules. Let $\beta\colon N \to N'$ and $\beta'\colon N' \to N''$ be homomorphisms of left R-modules.*

(a) *There exists a unique abelian group homomorphism $\alpha \otimes_R \beta\colon M \otimes_R N \to M' \otimes_R N'$ such that $(\alpha \otimes_R \beta)(m \otimes n) = \alpha(m) \otimes_R \beta(n)$ for all $m \in M$ and all $n \in N$.*
(b) *The following diagram commutes*

$$\begin{array}{ccc} M \otimes_R N & \xrightarrow{\alpha \otimes_R \beta} & M' \otimes_R N' \\ & \searrow^{(\alpha'\alpha) \otimes_R (\beta'\beta)} & \downarrow{\scriptstyle \alpha' \otimes_R \beta'} \\ & & M'' \otimes_R N'' \end{array}$$

In other words, we have $(\alpha' \otimes_R \beta')(\alpha \otimes_R \beta) = (\alpha'\alpha) \otimes_R (\beta'\beta)$.

PROOF. (a) We use the universal property. Define $f\colon M \times N \to M' \otimes_R N'$ by the formula $f(m,n) = \alpha(m) \otimes \beta(n)$. In other words, f is the composition $M \times N \xrightarrow{\alpha \times \beta} M' \times N' \xrightarrow{h'} M' \otimes_R N'$ where h' is the appropriate universal biadditive map. Since α and β are R-module homomorphisms, it is straightforward to show that f is R-biadditive. The universal property yields a unique abelian group homomorphism $\alpha \otimes_R \beta\colon M \otimes_R N \to M' \otimes_R N'$ such that

$$(\alpha \otimes_R \beta)(m \otimes n) = f(m,n) = \alpha(m) \otimes_R \beta(n)$$

for all $m \in M$ and all $n \in N$.

(b) By definition, we have

$$\begin{aligned}(\alpha' \otimes_R \beta')((\alpha \otimes_R \beta)(m \otimes n)) &= (\alpha' \otimes_R \beta')(\alpha(m) \otimes_R \beta(n)) \\ &= \alpha'(\alpha(m)) \otimes_R \beta'(\beta(n)) \\ &= (\alpha'\alpha) \otimes_R (\beta'\beta)(m \otimes n).\end{aligned}$$

Now apply Lemma 11.8(b). □

NOTATION 12.6. Continue with the notation of Proposition 12.5. We write

$$M \otimes_R \beta = \mathrm{id}_M \otimes_R \beta \colon M \otimes_R N \to M \otimes_R N'$$
$$\alpha \otimes_R N = \alpha \otimes_R \mathrm{id}_N \colon M \otimes_R N \to M' \otimes_R N.$$

REMARK 12.7. Let R be a ring. Let M be a right R-module and let N be a left R-module. It is straightforward to show that $\mathrm{id}_M \otimes_R N = \mathrm{id}_{M \otimes_R N} \colon M \otimes_R N \to M \otimes_R N$. Proposition 12.5(b) then shows that the operator $M \otimes_R -$ is a functor $R\text{-mod} \to \mathcal{A}b$. Similarly, one sees that $- \otimes_R N$ is a functor mod-$R \to \mathcal{A}b$. (Here mod-R is the category of right R-modules.) It is straightforward to show that the functors $M \otimes_R -$ and $- \otimes_R N$ are additive.

13. Day 13

Next, we go for exactness properties.

PROPOSITION 13.1. *Let $f \colon M \to M'$ be an epimorphism of right R-modules, and let $g \colon N \to N'$ be an epimorphism of left R-modules*

(a) *The map $f \otimes_R g \colon M \otimes_R N \to M' \otimes_R N'$ is surjective.*
(b) $\mathrm{Ker}(f \otimes_R g)$ *is generated as an abelian group by the set*

$$L = \{m \otimes n \in M \otimes_R N \mid f(m) = 0 \text{ or } g(n) = 0\} \subseteq M \otimes_R N.$$

PROOF. (a) We compute directly: For an arbitrary element $\sum_i m_i' \otimes n_i' \in M' \otimes_R N'$, we have

$$\textstyle\sum_i m_i' \otimes n_i' = \sum_i f(m_i) \otimes g(n_i) = (f \otimes_R g)(\sum_i m_i \otimes n_i).$$

(b) Let K denote the subgroup of $M \otimes_R N$ generated by the set L. Each generator of K is in $\mathrm{Ker}(f \otimes_R g)$, and so $K \subseteq \mathrm{Ker}(f \otimes_R g)$. Hence, we have a well-defined abelian group epimorphism $\phi \colon (M \otimes_R N)/K \to M' \otimes_R N'$ such that $\phi(\overline{m \otimes n}) = f(m) \otimes g(n)$. To show that $K = \mathrm{Ker}(f \otimes_R g)$, it suffices to show that ϕ is injective.

Define a map $h \colon M' \times_R N' \to (M \otimes_R N)/K$ as follows: for $(m', n') \in M' \times_R N'$, fix $m \in M$ and $n \in N$ such that $f(m) = m'$ and $g(n) = n'$, and set $h(m', n') = \overline{m \otimes n}$. We need to show this is well-defined. Assume $f(m_1) = m' = f(m)$ and $g(n_1) = n' = g(n)$. Then $m_1 - m \in \mathrm{Ker}(f)$ and $n_1 - n \in \mathrm{Ker}(g)$ and so in $M \otimes_R N$ we have

$$\begin{aligned}m_1 \otimes n_1 &= (m_1 - m) \otimes (n_1 - n) \\ &= \underbrace{(m_1 - m) \otimes (n_1 - n) + (m_1 - m) \otimes n + m \otimes (n_1 - n)}_{\in K} + m \otimes n.\end{aligned}$$

It follows that, in $(M \otimes_R N)/K$, we have $\overline{m_1 \otimes n_1} = \overline{m \otimes n}$ and so h is well-defined.

We check that h is R-biadditive. For instance, we want $h(m_1' + m_2', n') = h(m_1', n') + h(m_2', n')$. Fix $m_1, m_2 \in M$ and $n \in N$ such that $f(m_1) = m_1'$, $f(m_2) = m_2'$ and $g(n) = n'$. Then $f(m_1 + m_2) = m_1' + m_2'$ and so

$$h(m_1' + m_2', n') = \overline{(m_1 + m_2) \otimes n} = \overline{m_1 \otimes n} + \overline{m_2 \otimes n} = h(m_1', n') + h(m_2', n').$$

The other conditions are verified similarly.

Since h is R-biadditive, the universal property for tensor products yields a well-defined abelian group homomorphism $H\colon M' \otimes_R N' \to (M \otimes_R N)/K$ such that $H(m' \otimes n') = h(m', n')$ for all $m' \in M'$ and all $n' \in N'$. In other words,

$$H(m' \otimes n') = \overline{m \otimes n}$$

where $m \in M$ and $n \in N$ are such that $f(m) = m'$ and $g(n) = n'$. It follows readily that the composition $H\phi\colon (M \otimes_R N)/K \to (M \otimes_R N)/K$ is $\mathrm{id}_{(M \otimes_R N)/K}$, and so ϕ is injective as desired. □

Here is the right-exactness of the tensor product.

PROPOSITION 13.2. *Let R be a ring, M a right R-module and N a left R-module.*

(a) *The functor $M \otimes_R -\colon R\text{-mod} \to \mathcal{A}b$ is right exact: For each an exact sequence of left R-modules $N' \xrightarrow{g'} N \xrightarrow{g} N'' \to 0$ the associated sequence of abelian groups*

$$M \otimes_R N' \xrightarrow{M \otimes_R g'} M \otimes_R N \xrightarrow{M \otimes_R g} M \otimes_R N'' \to 0$$

is exact.

(b) *The functor $- \otimes_R N\colon \text{mod-}R \to \mathcal{A}b$ is right exact: For each an exact sequence of right R-modules $M' \xrightarrow{f'} M \xrightarrow{f} M'' \to 0$ the associated sequence of abelian groups*

$$M' \otimes_R N \xrightarrow{f' \otimes_R N} M \otimes_R N \xrightarrow{f \otimes_R N} M'' \otimes_R N \to 0$$

is exact.

PROOF. (a) Because g is surjective, Proposition 13.1(a) implies that $M \otimes_R g$ is surjective. Also, we have

$$(M \otimes_R g)(M \otimes_R g') = M \otimes_R (gg') = M \otimes_R 0 = 0$$

and so $\mathrm{Im}(M \otimes_R g') \subseteq \mathrm{Ker}(M \otimes_R g)$. To show $\mathrm{Im}(M \otimes_R g') \supseteq \mathrm{Ker}(M \otimes_R g)$, it suffices to show that every generator of $\mathrm{Ker}(M \otimes_R g)$ is in $\mathrm{Im}(M \otimes_R g')$. By Proposition 13.1(b), $\mathrm{Ker}(M \otimes_R g)$ is generated by $\{m \otimes n \mid g(n) = 0\}$. For each $m \otimes n \in M \otimes_R N$ such that $g(n) = 0$, there exists $n' \in N'$ such that $g'(n') = n$ and so $m \otimes n = (M \otimes_R g')(m \otimes n') \in \mathrm{Im}(M \otimes_R g')$.

Part (b) is similar. □

In general, the tensor product is not left exact.

EXAMPLE 13.3. Let $\mu\colon \mathbb{Z} \to \mathbb{Z}$ be the monomorphism given by $n \mapsto 2n$. It is straightforward to show that the following diagram commutes

$$\begin{array}{ccc} (\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z} & \xrightarrow[\cong]{F} & \mathbb{Z}/2\mathbb{Z} \\ \downarrow{\scriptstyle (\mathbb{Z}/2\mathbb{Z}) \otimes \mu} & & \downarrow{\scriptstyle \overline{\mu}} \\ (\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z} & \xrightarrow[\cong]{F} & \mathbb{Z}/2\mathbb{Z} \end{array}$$

where $\overline{\mu}(\overline{n}) = \overline{\mu(n)} = \overline{2n} = 0$. It follows that $\mu_2^{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathrm{id}_{\mathbb{Z}/2\mathbb{Z}} = 0$. This map is not injective because $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$.

DEFINITION 13.4. Let R be a ring. A right R-module M is *flat* if the functor $M \otimes_R -$ is exact. A left R-module N is *flat* if the functor $- \otimes_R N$ is exact.

EXAMPLE 13.5. Let R be a ring with identity. Then R is flat as a left R-module and as a right R-module. More generally any projective R-module is flat.

Our last topic is localization. It generalizes the construction of the field of fractions of an integral domain. It will also give us examples of flat R-modules that are not projective.

DEFINITION 13.6. Let R be a commutative ring with identity. A subset $S \subseteq R$ is *multiplicatively closed* if $1 \in S$ and $ss' \in S$ for all $s, s' \in S$.

Here are the prototypical examples of multiplicatively closed subsets.

EXAMPLE 13.7. Let R be a commutative ring with identity. For each $s \in R$, the set $\{1, s, s^2, \ldots\} \subseteq R$ is multiplicatively closed. For each prime ideal $\mathfrak{p} \subset R$, the set $R \smallsetminus \mathfrak{p} \subset R$ is multiplicatively closed. For instance, if R is an integral domain, then the set of nonzero elements of R is multiplicatively closed.

CONSTRUCTION 13.8. Let R be a commutative ring with identity, and let $S \subseteq R$ be multiplicatively closed. Define a relation $\sim$ on $R \times S$ as follows: $(r, s) \sim (r', s')$ if there exists $s'' \in S$ such that $s''(rs' - r's) = 0$. Check that this is an equivalence relation on $R \times S$.

The *localization* $S^{-1}R$ is then the set of all equivalence classes under this relation $S^{-1}R = (R \times S)/\sim$ where the equivalence class of (r, s) in $S^{-1}R$ is denoted r/s or $\frac{r}{s}$. If $t \in S$, then the definition implies $(r, s) \sim (rt, st)$; this translates to the cancellation formula $\frac{rt}{st} = \frac{r}{s}$.

For elements $r/s, t/u \in S^{-1}R$, set

$$\frac{r}{s} + \frac{t}{u} = \frac{ru + ts}{su} \qquad \text{and} \qquad \frac{r}{s}\frac{t}{u} = \frac{rt}{su}.$$

When $\mathfrak{p} \subset R$ is a prime ideal and $S = R \smallsetminus \mathfrak{p}$, we write $R_{\mathfrak{p}}$ in lieu of $S^{-1}R$.

EXAMPLE 13.9. Let R be an integral domain, and set $S = \{r \in R \mid r \neq 0\}$. Then $S^{-1}R$ is the quotient field of R.

PROPOSITION 13.10. *Let R be a commutative ring with identity, and let $S \subseteq R$ be multiplicatively closed.*

(a) *$S^{-1}R$ is a commutative ring with identity, with $0_{S^{-1}R} = 0_R/1_R = 0/s$ and $1_{S^{-1}R} = 1_R/1_R = s/s$ for all $s \in S$.*
(b) *The assignment $f\colon R \to S^{-1}R$ given by $r \mapsto r/1$ is a homomorphism of rings with identity.*

PROOF. Argue as in the proof of Proposition 11.16. The main point is to show that the addition and multiplication on $S^{-1}R$ are well-defined; the other ring-axioms are then easily verified. Assume that $r/s = r'/s'$ and $t/u = t'/u'$, that is, $s''(rs' - r's) = 0 = u''(tu' - t'u)$ for some $s'', u'' \in S$. Then

$$\begin{aligned}\frac{ru + ts}{su} &= \frac{(ru + ts)s's''u'u''}{(su)s's''u'u''} = \frac{rs's''uu'u'' + tu'u''ss's''}{ss's''uu'u''} \\ &= \frac{r'ss''uu'u'' + t'uu''ss's''}{ss's''uu'u''} = \frac{(r'u' + t's)ss''uu''}{(s'u')ss''uu''} = \frac{r'u' + t's}{s'u'}\end{aligned}$$

so addition is well-defined. The equality $\frac{rt}{su} = \frac{r't'}{s'u'}$ is even easier to verify, showing that multiplication is well-defined. □

CONSTRUCTION 13.11. Let R be a commutative ring with identity, and let $S \subseteq R$ be multiplicatively closed. Let M be a unital R-module. Define a relation $\sim$ on $M \times S$ as follows: $(m, s) \sim (m', s')$ if there exists $s'' \in S$ such that $s''(ms' - m's) = 0$. Check that this is an equivalence relation on $M \times S$.

The *localization* $S^{-1}M$ is then the set of all equivalence classes under this relation $S^{-1}M = (M \times S)/\sim$ where the equivalence class of (m, s) in $S^{-1}M$ is denoted m/s or $\frac{m}{s}$. If $t \in S$, then the definition implies $(m, s) \sim (tm, ts)$; this translates to the cancellation formula $\frac{tm}{ts} = \frac{m}{s}$.

For elements $m/s, n/u \in S^{-1}M$ and $r/v \in S^{-1}R$, set

$$\frac{m}{s} + \frac{n}{u} = \frac{um + sn}{su} \qquad \text{and} \qquad \frac{r}{v}\frac{m}{s} = \frac{rm}{vs}.$$

When $\mathfrak{p} \subset R$ is a prime ideal and $S = R \smallsetminus \mathfrak{p}$, we write $M_{\mathfrak{p}}$ in lieu of $S^{-1}M$.

PROPOSITION 13.12. *Let R be a commutative ring with identity, and let $S \subseteq R$ be multiplicatively closed. Let $f\colon M \to N$ be a homomorphism of unital R-modules.*

(a) *$S^{-1}M$ is a unital $S^{-1}R$-module, with $0_{S^{-1}M} = 0_M/1_R = 0_M/s$ for all $s \in S$.*
(b) *$S^{-1}M$ is a unital R-module, with action $r(m/s) = (rm)/s$.*
(c) *The assignment $g_M\colon M \to S^{-1}M$ given by $m \mapsto m/1$ is a homomorphism of unital R-modules.*
(d) *The assignment $S^{-1}f\colon S^{-1}M \to S^{-1}N$ given by $m/s \mapsto f(m)/s$ is a homomorphism of unital $S^{-1}R$-modules making the following diagram commute*

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle g_M}\downarrow & & \downarrow{\scriptstyle g_N} \\ S^{-1}M & \xrightarrow{S^{-1}f} & S^{-1}N. \end{array}$$

(e) *The operator $S^{-1}(-)\colon R\text{-mod} \to S^{-1}R\text{-mod}$ is an exact additive covariant functor.*

PROOF. Parts (a) and (b) are proved as in Proposition 13.10. Most of the remaining parts are exercises in applying the definitions. We explain the well-definedness of $S^{-1}f$ and the exactness of $S^{-1}(-)$.

To see that $S^{-1}f$ is well-defined, let $m/s = n/t \in S^{-1}M$. Then there exists $u \in S$ such that $utm = usn$, and so

$$utf(m) = f(utm) = f(usn) = usf(n).$$

It follows that

$$\frac{f(m)}{s} = \frac{utf(m)}{uts} = \frac{usf(n)}{ust} = \frac{f(n)}{t}$$

in $S^{-1}N$, as desired.

To see that $S^{-1}(-)$ is exact, consider an exact sequence of R-modules

$$M \xrightarrow{f} N \xrightarrow{g} L.$$

We need to show that the sequence

$$S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}L$$

is exact. The functoriality of $S^{-1}(-)$ implies

$$(S^{-1}g) \circ (S^{-1}f) = S^{-1}(g \circ f) = S^{-1}(0) = 0$$

and so $\operatorname{Im}(S^{-1}f) \subseteq \operatorname{Ker}(S^{-1}g)$. For the reverse containment, let $n/s \in \operatorname{Ker}(S^{-1}g)$. Then

$$0/1 = 0 = (S^{-1}g)(n/s) = g(n)/s$$

so there exists $t \in S$ such that

$$g(tn) = tg(n) = ts0 = 0.$$

The exactness of the original sequence yields an element $m \in M$ such that $f(m) = tn$. It follows that

$$n/s = tn/ts = f(m)/ts = (S^{-1}f)(m/ts) \in \operatorname{Im}(S^{-1}f)$$

as desired. □

PROPOSITION 13.13. *Let R be a commutative ring with identity, and let $S \subseteq R$ be multiplicatively closed. Let M be a unital R-modules.*

(a) *Every element of $(S^{-1}R) \otimes_R M$ is of the form $\frac{r}{s} \otimes m$ for some $r \in R$ and $s \in S$ and $m \in M$.*
(b) *There is a natural isomorphism of functors $S^{-1}R \otimes_R - \cong S^{-1}(-)\colon R\text{-}mod \to \mathcal{A}b$.*
(c) *$S^{-1}R$ is a flat R-module.*

PROOF. (a) Fix an element $\sum_i \frac{r_i}{u_i} \otimes m_i \in (S^{-1}R) \otimes_R M$. Set $u = \prod_i u_i$ and $u_i' = \prod_{j \neq i} u_j$. Then $u = u_i' u_i$ and so

$$\textstyle\sum_i \frac{r_i}{u_i} \otimes m_i = \sum_i \frac{u_i' r_i}{u_i' u_i} \otimes m_i = \sum_i \frac{1}{u} \otimes (u_i' r_i m_i) = \frac{1}{u} \otimes \left(\sum_i u_i' r_i m_i\right).$$

(b) The universal mapping property for tensor products shows that the map $F\colon S^{-1}R \otimes_R M \to S^{-1}M$ given by $F\left(\frac{r}{u} \otimes m\right) = \frac{rm}{u}$ is a well-defined abelian group homomorphism. The map F is surjective: $\frac{m}{u} = F\left(\frac{1}{u} \otimes m\right)$. To see that F is injective, fix $\xi \in \operatorname{Ker}(F)$. Part (a) implies that $\xi = \frac{r}{u} \otimes m$ for some $r \in R$ and $u \in S$ and $m \in M$. Then $0 = F\left(\frac{r}{u} \otimes m\right) = \frac{rm}{u}$ implies that there exists an element $u' \in S$ such that $u'rm = 0$. Hence, we have

$$\frac{r}{u} \otimes m = \frac{ru'}{uu'} \otimes m = \frac{1}{uu'} \otimes (ru'm) = \frac{1}{uu'} \otimes (0) = 0.$$

To show that the isomorphism is natural, let $g\colon M \to M'$ be an R-module homomorphism. We need to show that the following diagram commutes:

$$\begin{array}{ccc} (S^{-1}R) \otimes_R M & \xrightarrow{(S^{-1}R) \otimes g} & (S^{-1}R) \otimes_R M' \\ \cong \big\downarrow F & & \cong \big\downarrow F' \\ S^{-1}M & \xrightarrow{\quad S^{-1}g \quad} & S^{-1}M' \end{array}$$

where the vertical maps are the isomorphisms from the previous paragraph. We have $S^{-1}g\big(\frac{m}{u}\big) = \frac{g(m)}{u}$, and so

$$\begin{aligned} F'(((S^{-1}R) \otimes_R g)(\tfrac{r}{u} \otimes m)) &= F'(\tfrac{r}{u} \otimes g(m)) \\ &= \tfrac{rg(m)}{u} \\ &= \tfrac{g(rm)}{u} \\ &= (S^{-1}g)(\tfrac{rm}{u}) \\ &= (S^{-1}g)(F(\tfrac{r}{u} \otimes m)). \end{aligned}$$

(c) The functor $S^{-1}(-) \cong (S^{-1}R) \otimes_R -$ is exact by Proposition 13.12(e), and so $S^{-1}R$ is flat by definition. □