MATH 3322 Problem Set 6

March 19, 2019

Solutions

Question 1. By the primitive element theorem, Theorem 8, a primitive element for $K(\theta_1, \theta_2)$ can be found in the form $\theta_1 + k\theta_2$ for some $k \in K$. For instance, it is easy to see that $\sqrt{2}+i$ is a primitive element for $\mathbb{Q}(\sqrt{2}, i)$. For $(\sqrt{2}+i)^2 = 1 + 2i\sqrt{2}$, and so $\sqrt{2}i \in \mathbb{Q}(\sqrt{2}+i)$. But then $(\sqrt{2}+i)(\sqrt{2}i) = 2i - \sqrt{2} \in \mathbb{Q}(\sqrt{2}+i)$, from which it follows easily that both $i \in \mathbb{Q}(\sqrt{2}+i)$ and $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+i)$.

Find a primitive element (with explanation) for each of

[2] (a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$;

Solution: The example suggests a solution to this by taking $\theta = \sqrt{2}+\sqrt{3}$. For then $\theta^2 = 2 + \sqrt{2}\sqrt{3} + 3$, and so $\sqrt{2}\sqrt{3} \in \mathbb{Q}(\theta)$. But then $\theta\sqrt{2}\sqrt{3} = 2\sqrt{3} + 3\sqrt{2}$ and it follows easily that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\theta)$.

Solution: Notice that $(\sqrt{2}+\sqrt{3})(\sqrt{3}-\sqrt{2}) = 1$, so $\sqrt{3}-\sqrt{2} = (\sqrt{2}+\sqrt{3})^{-1} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. So immediately, $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

[4] (b) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

Solution: There is an easy solution here if the inspiration strikes you.

Clearly $\theta = \sqrt{2}/\sqrt[3]{2} = \sqrt[6]{2} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

But $\sqrt{2} = \left(\sqrt[6]{2}\right)^3$ and $\sqrt[3]{2} = \left(\sqrt[6]{2}\right)^2$, so $\mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

Solution: $\theta = \sqrt{2} + \sqrt[3]{2}$ is also a primitive element.

How to prove it?

Thanks to W.Z. for the following elegant solution:

Notice that $(\theta - \sqrt{2})^3 = 2$, so $\theta^3 - 3\theta^2\sqrt{2} + 6\theta - 2\sqrt{2} = 2$.

Solving for $\sqrt{2}$ yields

$$\sqrt{2} = \frac{\theta^3 + 6\theta - 2}{3\theta^2 + 2},$$

so $\sqrt{2} \in \mathbb{Q}(\theta)$, and so also $\sqrt[3]{2} = \theta - \sqrt{2} \in \mathbb{Q}(\theta)$.

Question 2. Let K/F be a field extension, R a ring, and $F \leq R \leq K$.

[2] (a) Suppose that K/F is algebraic.

Prove that R is a field.

Proof: Let $\alpha \in R$. But α is the root of some polynomial over F, say of degree $n \geq 1$, and we have seen that the elements of the field $F(\alpha)$ all can be written as polynomials in α of degree $< n$. Therefore $F(\alpha) \subseteq R$, in particular, $\alpha^{-1} \in R$. So R is a field ∎

[2] (b) Give an example to show that the result fails when K/F is not algebraic.

Solution: I think every example works. For instance $F \subseteq F[x] \subseteq F(x)$ is typical.

Yes! Suppose that for every intermediate ring $F \leq R \leq K$, R is a field. Then in particular, for every $\alpha \in K$, $F[\alpha]$ is a field, so $\alpha^{-1} = q(\alpha)$ for some $q \in F[x]$. Then $\alpha q(\alpha) = 1$, so α is a root of the polynomial $xq(x) - 1$.

Question 3. Let $[K : F] = n$. Prove the following:

[2] (a) For all $\alpha \in K$, $\phi_\alpha : K \to K : k \mapsto \alpha k$ is a linear transformation of the vector space ${}_F K$.

Proof: This is nothing more than saying that field multiplication is commutative, and distributive over addition.

Let k_1, k_2 be elements of K and $a \in F$.

Then $\phi_\alpha(ak_1 + k_2) = \alpha(k_1 + k_2) = \alpha a k_1 + \alpha k_2 = a\alpha k_1 + \alpha k_2 = a\phi_\alpha(k_1) + \phi_\alpha(k_2)$, so ϕ_a is linear. ∎

[2] (b) The map defined by sending each $\alpha \in K$ to the matrix of the linear transformation ϕ_α is an embedding of K as a subfield of the ring $\mathsf{M}_n(F)$ of $n \times n$ matrices over F.

Proof: We know that the ring of linear transformations of a finite dimensional vector space to itself can be represented as $\mathsf{M}_n(F)$; so all that we need to observe is that $\phi_\alpha \circ \phi_\beta = \phi_{\alpha\beta}$ and $\phi_\alpha + \phi_\beta = \phi_\alpha + \phi_\beta$. Clearly if $\alpha \neq \beta$ then $\phi_\alpha \neq \phi_\beta$, so we have an embedding. ∎

(Hence every extension of F of degree n embeds as a subfield of $\mathsf{M}_n(F)$.

Question 4. Each of $p_2 = x^2 + x + 1$, $p_3 = x^3 + x + 1$, and $p_4 = x^4 + x + 1$ is irreducible over $\mathbb{F}_2$, the field with two elements. Let α be a root of p_2, let β be a root of p_3, and let γ be a root of p_4.

[3] (a) Find all the roots of p_2 in $E_2 = \mathbb{F}_2(\alpha)$, all the roots of p_3 in $E_3 = \mathbb{F}_2(\beta)$, and all the roots of p_4 in $E_4 = \mathbb{F}_2(\gamma)$.

Solution: Trial and error is completely acceptable, but here is a detailed analysis:

All coefficients a in the following are in $\mathbb{Z}_2$, that is, are either 0 or 1, and so $a^2 = a$. Recall that $(x+y)^2 = x^2 + y^2$ in a field of characteristic 2.

Remember also that in E_2, every element will be a linear polynomial in α, in E_3 every element will be a quadratic polynomial in β, and in E_4, every element will be a third degree polynomial in γ, and we have the identities $\alpha^2 = \alpha + 1$, $\beta^3 = \beta + 1$, and $\gamma^4 = \gamma + 1$.

Furthermore, p_2 can have no more than 2 roots, p_3 can have no more than 3 roots, and p_4 can have no more than 4 roots.

And finally we take advantage of the squaring relationship mentioned at the beginning. Consider a root δ of a polynomial of the form $x^n + x + 1$ over $\mathbb{F}_2$,. So in some extension field E_n, $0 = \delta^n + \delta + 1$. Therefore

$$0 = 0^2 = (\delta^n + \delta + 1)^2 = \delta^{2n} + \delta^2 + 1\,,$$

so δ^2 is also a root. (!)

Therefore the roots are δ, δ^2, δ^4, $\ldots \delta^{2^{n-1}}$.

The roots of p_2 are α and $\alpha^2 = \alpha + 1$; the roots of p_3 are β, β^2, and $\beta^4 = \beta^2 + \beta$; and the roots of p_4 are γ, γ^2, $\gamma^4 = \gamma + 1$, and $\gamma^8 = \gamma^2 + 1$.

Solution: Trial-and-error is not too bad for p_3, but is awkward already for p_4. But we can do a systematic search even without the insight used in the previous solution. Take a typical element of E_4, say $\delta = a_3\gamma^3 + a_2\gamma^2 + a_1\gamma + a_0$. Then $\delta^4 = a_3\gamma^{12} + a_2\gamma^8 + a_1\gamma^4 + a_0 = a_3(\gamma^3 + \gamma^2 + \gamma + 1) + a_2(\gamma^2 + 1) + a_1(\gamma + 1) + a_0$ and so $p_3(\delta) = a_3(\gamma^3 + \gamma^2 + \gamma + 1 + \gamma^3) + a_2(\gamma^2 + 1 + \gamma^2) + a_1(\gamma + 1 + \gamma) + a_0 + a_0 + 1 = a_3(\gamma^2 + \gamma) + a_3 + a_2 + a_1 + 1$.

So $p_3(\delta) = 0$ iff $a_3 = 0$ and $a_3 + a_2 + a_1 + 1 = 0$, that is $a_3 = 0$ and $a_2 + a_1 + 1 = 0$; giving the four solutions γ, γ^2, $\gamma + 1$, and $\gamma^2 + 1$.

[1] (b) Give a brief explanation of why E_2 does not embed in E_3 and of why E_3 does not embed in E_4.

Solution: The cardinalities of the group of units of each of these three fields are 3, 7, 15 respectively, and 3 does not divide 7 and 7 does not divide 15.

Alternatively, $[E_4 : \mathbb{F}_2] = 4$, $[E_3 : \mathbb{F}_2] = 3$, and $[E_2 : \mathbb{F}_2] = 2$, and $2 \nmid 3$, $3 \nmid 4$.

[2] (c) Show that the map determined by $\alpha \mapsto \gamma^2 + \gamma + 1$ defines an embedding of $E_2 \hookrightarrow E_4$.

Proof: p_2 is an irreducible polynomial and α is a root. Observe that $p_2(\gamma^2 + \gamma + 1) = (\gamma^2 + \gamma + 1)^2 + (\gamma^2 + \gamma + 1) + 1 = (\gamma^4 + \gamma^2 + 1) + (\gamma^2 + \gamma + 1) + 1 = 0$. Therefore $E_2 = \mathbb{F}_2(\alpha) \cong \mathbb{F}_2(\gamma^2 + \gamma + 1) \subseteq \mathbb{F}_2(\gamma) = E_4$. ∎