University of Manitoba

Department of Mathematics

Rings and Modules Seminar
~ Abstracts ~

R. Padmanabhan and A. Clay
Ranganathan(dot)Padmanabhan(at)umanitoba(dot)ca
Adam(dot)Clay(at)umanitoba(dot)ca

University of Manitoba

Tuesday, March 07, 14, 2023

Analogs of Mumford-Ramanujam Theorem for Universal Algebras
Part I: History and Examples
Part II: Structure Theorems

Analogs of Mumford-Ramanujam Theorem for Universal Algebras
Part I: History and Examples
Part II: Structure Theorems

Abstract:

A well-known result in quasigroup theory says that an associative quasigroup is a group, i.e. in quasigroups, associativity forces the existence of an identity element. The converse is, of course, far from being true, as there are many, many non-associative loops. However, a remarkable theorem due to David Mumford and C.P. Ramanujam says that in a projective variety V, if a binary law of composition m merely possessed a 2-sided identity $m(x, e) = m(e, x) = x$, then m must also have an inverse and satisfy the associative law, hence make V into a group. Motivated by this result, we define a universal algebra $(A;\ F)$ to be an MR-algebra if whenever a binary term-function $m(x, y)$ admits a two-sided identity, then the reduct $(A, m(x, y))$ must be associative. Here we give some non-trivial varieties of quasigroups, groups, rings, fields and lattices which are MR-algebras. For example, every MR-quasigroup must be isotopic to a group, MR-groups are exactly the nilpotent groups of class 2, while commutative rings and complemented lattices are MR-algebras if and only if they are Boolean.

C. P. Ramanujam proved that if a binary operation m in a complete variety X merely possessed a 2-sided identity then m must have an inverse and satisfy the associative law, hence make X into a group ! We look at this as a formal implication:

$$m(x, e) = \mathrm{m}(e, x) = x \text{ implies } m(m(x, y), z) = \mathrm{m}(x, \mathrm{m}(y, z)).$$

Some examples of binary algebras having a two-sided identity and inverse but not associative

1. The most famous non-associative Moufang loop is the multiplicative loop of real octonions.

2. The binary algebra ($\mathbb{R}$; *) where $x*y = x + y + x^2y$ is a ***polynomially defined*** algebra having a 2-sided identity but not associative.

3. The binary algebra ($\mathbb{N}$; *) where $x*y = x^y y^x$ is commutative, has a 2-sided identity but not associative.

$\circ$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	7	5	0	6	2	4	3
2	2	6	7	5	0	3	1	4
3	3	0	6	7	5	4	2	1
4	4	5	0	6	7	1	3	2
5	5	2	3	4	1	7	0	6
6	6	4	1	2	3	0	7	5
7	7	3	4	1	2	6	5	0

Here 0 is the identity, and the inverses are $0, 3, 4, 1, 2, 6, 5, 7$ for $0 \ldots 7$ respectively. Consider $1 \circ 1 \circ 2$ to show non-associativity and $1 \circ 2$ for non-commutativity.

Theorem.

Let $x \oplus y = ax^2 + hxy + by^2 + fx + gy + c$ *in* $k[x, y]$ for some infinite field k. If $\oplus$ admits a two-sided identity, then it is associative.

Proof.

Let $x \oplus e = e \oplus x = x$ *for some* e *in* k. *Now* $x + e = x$ *implies that* $ax^2 + hxe + be^2 + fx + ge + c = x$. *Since* k *is an infinite field, we have* $a = 0$, $he + f = 1$, *and similarly,* $b = 0$, $he + g = 1$. *In particular, we get* $f = g$. *Rewriting the binary operation* $\oplus$ *in its new simplified form we have* $x \oplus y = axy + bx + by + c$. *for some* a, b, c *in* k. *and also* $ae + b = 1$ *and* $be + c = 0$. *If* $a = 0$, *then* $b = 1$ *and* $x \oplus y$ *is the usual addition which is, of course, is associative. Let now* $a \neq 0$. *Then* $c = -be = -bae/a = -b(1-b)/a = (\underline{b}^2 - b)/a$. *Thus we have the final form*

$$x \oplus y = axy + bx + by + (b^2 - b)/a.$$

$$(x \oplus y) \oplus z = a^2xyz + ab(xy+yz+zx) + b^2(x+y+z) + bc+c$$

which is symmetric in x, y *and* z. *So* $+$ *is associative.*

In simple terms, Rigidity Lemma (see p 44 - 45) says that under certain circumstances "a 2-variable function f (x, y) that is independent of x for one value of y is independent of x for all y.

$$\boxed{\text{M-R, Theorem. } m(x,e) = m(e,x) \Longrightarrow m(x,m(y,z)) = m(m(x,y),z)}$$

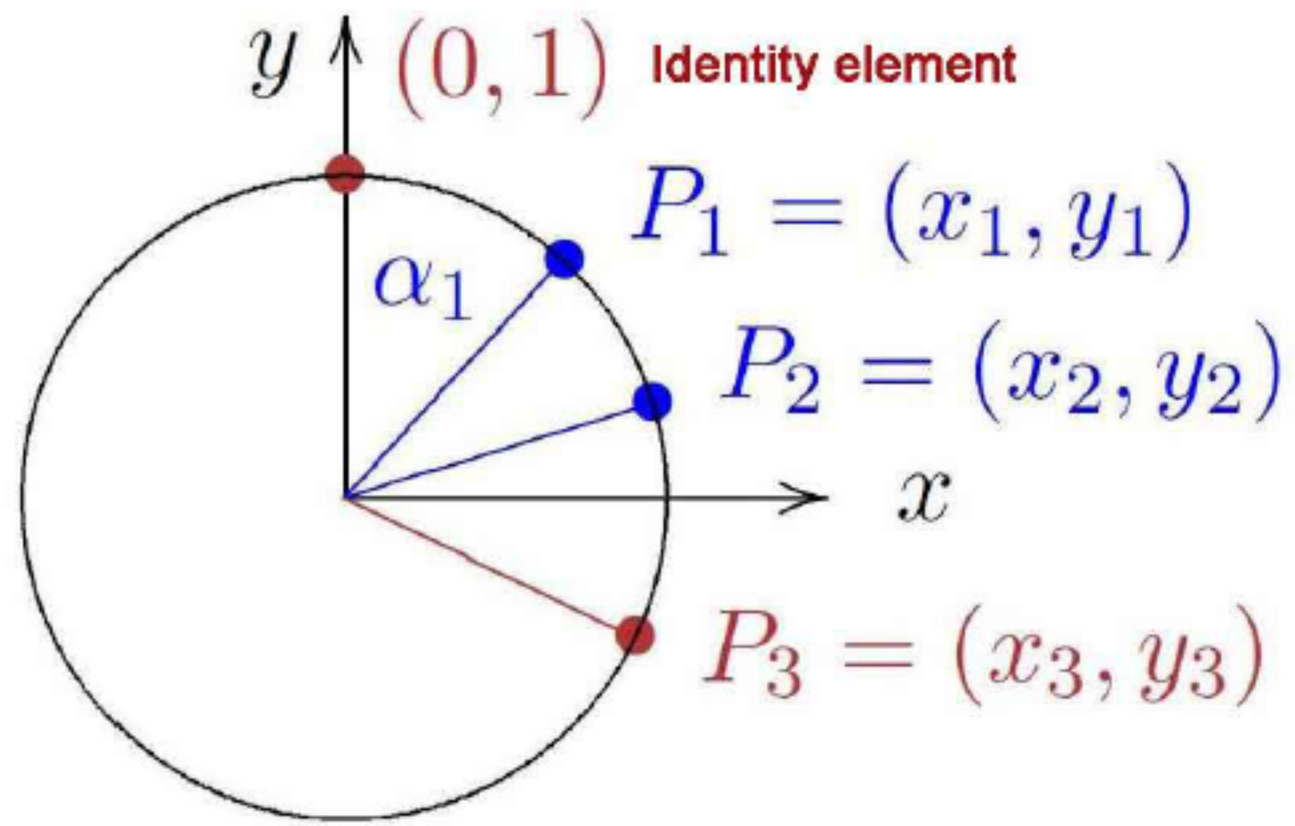
Key steps of the proof (for complete details, see pages 45-46 of [9].
Let A be the projective curve. Define f:A x A —> A x A by the rule $f(x,y) = (xy, y)$. Now $f(e, e) = (e, e)$. Conversely, if $f(x, y) = (e, e)$, then $(xy, y) = (e, e)$ which, in trun, implies that $x=e$, $y=e$. In other words, $f^{-1}(e, e) = \{(e, e)\}$.Using this and the fact we have a projective curve, CPR proves that the mapping is onto and thus captures the inverse, y' from $(xy, y) = (e,y)$ for some x i.e. given y, the equation $xy=e$ is soluble for x so that we have $x'x = e$. Then he goes on to prove other familiar properties like $y'' = y$, $yy' = e$ etc. Next, he uses the rigidity lemma to the binary term-function $x'(xy)$ to conclude that $x'(xy) = y$. Finally, applying rigidity to the ternary term function $x(x'y)z)$ he gets full associativity.

Let $x^2 + y^2 = 1$ be the unit circle equation and $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ b
points on this circle. We have

$$(x_1, y_1) = (sin(\alpha_1), cos(\alpha_1)), \quad (x_2, y_2) = (sin(\alpha_2), cos(\alpha_2))$$

and thus this addition is given by

$$\begin{aligned} x_3 &= sin(\alpha_1 + \alpha_2) \\ &= sin(\alpha_1)cos(\alpha_2) + cos(\alpha_1)sin(\alpha_2) \\ &= x_1y_2 + y_1x_2 \\ y_3 &= cos(\alpha_1 + \alpha_2) \\ &= cos(\alpha_1)cos(\alpha_2) - sin(\alpha_1)sin(\alpha_2) \\ &= y_1y_2 - x_1x_2 \end{aligned}$$



Group Law on Unit Circle

$$
\begin{aligned}
x_3 &= \sin(\alpha_1 + \alpha_2) \\
&= \sin(\alpha_1)\cos(\alpha_2) + \cos(\alpha_1)\sin(\alpha_2) \\
&= x_1 y_2 + x_2 y_1
\end{aligned}
$$

$$
\begin{aligned}
y_3 &= \cos(\alpha_1 + \alpha_2) \\
&= \cos(\alpha_1)\cos(\alpha_2) + \sin(\alpha_1)\sin(\alpha_2) \\
&= y_1 y_2 - x_1 x_2
\end{aligned}
$$

As introduced in the previous section, when $dx_1x_2y_1y_2 \neq \pm 1$, the group law on Edwards curves is given in the next algorithm:

Group law algorithm 3.2. *Let E_d be an* ***Edwards curve*** *given by:*

$$E_d : x^2 + y^2 = 1 + dx^2y^2$$

Let $P_0 = (x_0, y_0) \in E_d$, then $-P_0 = (-x_0, y_0)$. Now, let $P_1 + P_2 = P_3$ with $P_i = (x_i, y_i) \in E_d$ for $i = 1, 2, 3$. Then:

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

Here, the point $(0, 1)$ is the identity element and $-(x_1, y_1) = (-x_1, y_1)$,

Since the binary rational $+$ has a two-sided identity, viz. (0,1), by Mumford-Ramanujam , the addition is associative.

Group Law on Edwards Curves

Projective homogeneous coordinates [edit]

In the context of cryptography, homogeneous coordinates are used to prevent field inversions that appear in the affine formula. To avoid inversions in the original Edwards addition formulas, the curve equation can be written in projective coordinates as:

$$(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2.$$

A projective point $(X : Y : Z)$ corresponds to the affine point $(X/Z : Y/Z)$ on the Edwards curve.

The identity element is represented by $(0 : 1 : 1)$. The inverse of $(X : Y : Z)$ is $(-X : Y : Z)$.

The addition formula in homogeneous coordinates is given by:

$$(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$$

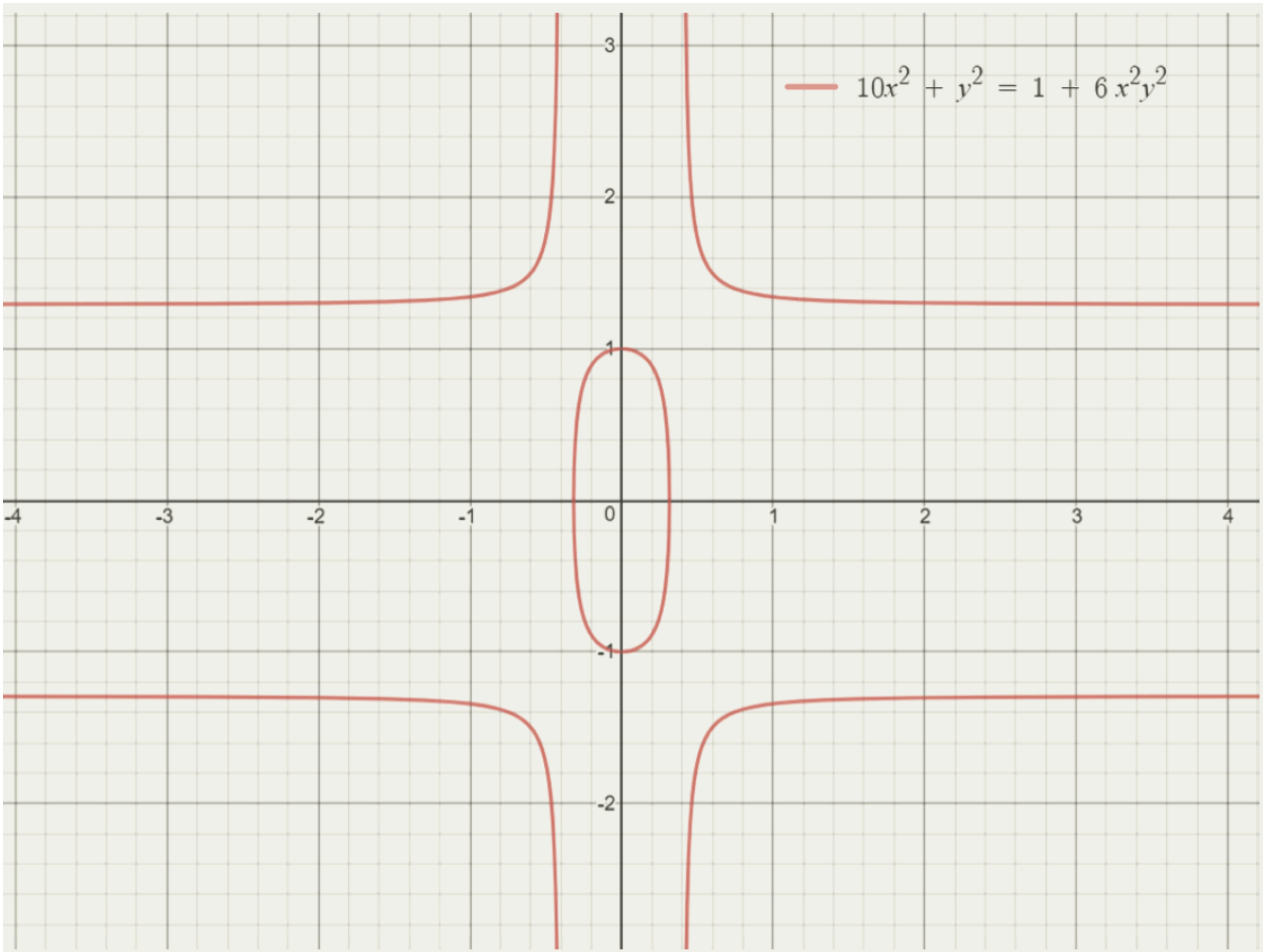
where

$$X_3 = Z_1Z_2(X_1Y_2 + X_2Y_1)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)$$

$$Y_3 = Z_1Z_2(Y_1Y_2 - X_1X_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)$$

$$Z_3 = (Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)$$

Here the point N = (0,1,1) is the identity. Let us verify: (x, y, z) + (0,1,1) = (xz^2, yz^2, z^3) = (x, y, z). Hence the operation defined on the left is associative.


$10x^2 + y^2 = 1 + 6x^2y^2$
3
2
1
-1
-2
-4
-3
-2
-1
0
1
2
3
4

References:

1. Garrett Birkhoff, **Lattice Theory**. Third edition. American Mathematical Society Colloquium Publications, Vol. XXV. American Mathematical Society, Providence, R.I., 1967.
2. Joel V. Brawley, Shuhong Gao, and Donald Mills, *Associative rational functions in two variables*, In **Finite Fields and Applications** (Augsburg, 1999), 43–56. Springer, Berlin, 2001.
3. T. Evans, *A note on the associative law*, **J. London Math. Soc.**, (25) 196–201, 1950.
4. S. Fajtlowicz, *On fundamental operations in groups*, **J. Austral. Math. Soc.**, (14) 445–447, 1972.
5. K. Glazek and B. Gleichgewicht, *On 3-semigroups and 3-groups polynomial-derived from integral domains*, **Semigroup Forum**, (32(1)) 61–70, 1985.
6. George Grätzer, **Universal algebra**. Springer, New York, second edition, 2008.
7. Lowell A. Hinrichs, Ivan Niven, and C. L. Vanden Eynden, *Fields defined by polynomials*, **Pacific J. Math.**, (14) 537–545, 1964.
8. A. Hulanicki and S. Swierczkowski, *On group operations other than xy or yx*, **Publ. Math. Debrecen**, (9) 142–148, 1962.
9. David Mumford, **Abelian varieties**. vol. 5, Tata Institute of Fundamental Research Studies in Mathematics, New Delhi, 2008.
10. Hanna Neumann, *On a question of Kertesz*, **Publ. Math. Debrecen**, (8) 75–78, 1961.
11. Robert W. Quackenbush, *Quasi-ane algebras*, **Alg. Universalis**, (20(3)) 318–327, 1985.