CRYPTOGRAPHY TOPIC VI
ALGEBRAIC CATEGORIES
DRAFT

PAUL L. BAILEY

Abstract. We define binary operations on a given set, magmas, monoids, groups, rings, fields, and the ring of polynomials over a field. We discuss how the division algorithm for the integers and for polynomials produces an analogy between $\mathbb{Z}$ and $F[x]$, and how this leads to the analogy between $\mathbb{Z}_p$ and other finite fields. We pick and choose the theory which will be helpful for cryptography.

1. Magmas

1.1. **Binary Operations.** Algebra is the study of binary operations. We give the precise definition and some examples.

Definition 1. Let A be a set. A *binary operation* on A is a function

$$* : A \times A \to A.$$

If $a_1, a_2 \in A$, we write $a_1 * a_2$ to mean $*(a_1, a_2)$.

We list our main examples.

Example 1. Let A be any of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then addition ($+$), subtraction ($-$), and multiplication ($\cdot$) are binary operations on A.

Example 2. Let A be any of $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, or $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Then division ($/$) is a binary operation on A.

Example 3. Let n be a positive integer. Then modular addition and multiplication are binary operations on $\mathbb{Z}_n$. If $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid a \text{ is invertible}\}$, we may define division on $\mathbb{Z}_n$ by $a/b = ab^{-1}$. Then division becomes a binary operation on $\mathbb{Z}_n^*$.

Example 4. Let $\mathbb{R}^n$ denote the set ordered n-tuples of real numbers, viewed as vectors in n-dimensional space. Then vector addition is a binary operation on $\mathbb{R}^n$.

Example 5. Let $\mathbb{R}^3$ denote the set of vectors in three dimensional space. Then cross product ($\times$) is a binary operation on $\mathbb{R}^3$.

Note that dot product is not a binary operation on $\mathbb{R}^3$, because the dot product of two vectors is a real number, not a vector.

Example 6. Let X be a set and let $\mathcal{P}(X) = \{A \mid A \subset X\}$; this is the *power set* of X. Then union ($\cup$), intersection ($\cap$), complement ($\setminus$), and symmetric difference ($\triangle$) are binary operations on $\mathcal{P}(X)$. Note that if $|X| = n$, then $|\mathcal{P}(X)| = 2^n$ (why?).

Example 7. Let X be a set and let $\mathrm{Sym}(X) = \{f : X \to X \mid f \text{ is bijective}\}$. Then composition ($\circ$) is a binary operation on $\mathrm{Sym}(X)$. Note that if $|X| = n$, then $|\mathrm{Sym}(X)| = n!$ (why?).

Date: November 14, 2007.

1.2. **Magmas.** Algebraists classify binary operations on a given sets in an increasingly more specific sequence of properties. The binary operation and its properties are considered to be additional structure on the set. A set together with additional structure is referred to as an *object*. The class of all objects with a ceratin type of additional structure is known as a *category*. If this additional structure involves binary operations, we have an *algebraic category*. The simplest case of this is the magma.

Definition 2. A *magma* $(A, *)$ consists of a nonempty set A together with a binary operation $*$ on A.

Definition 3. Let $(A, *)$ be a magma.

We say that $*$ is *commutative* (or that $(A, *)$ is commutative) if

$$a * b = b * a \quad \text{for all} \quad a, b \in A.$$

We say that $*$ is *associative* (or that $(A, *)$ is associative) if

$$a * (b * c) = (a * b) * c \quad \text{for all} \quad a, b, c \in A.$$

Example 8. The magmas $(\mathbb{Z}, +)$, $(\mathbb{R}, \cdot)$, and $(\mathcal{P}(X), \cap)$ are commutative and associative.

The magma $(\mathrm{Sym}(X), \circ)$ is associative, but not commutative.

The magma $(\mathbb{Z}, -)$ is neither associative nor commutative.

Definition 4. Let $(A, *)$ be a magma.

Let $e \in A$. We say that e is an *identity* for $*$ if

$$a * e = e * a = a \quad \text{for all } a \in A.$$

Proposition 1. *Let $(A, *)$ be a magma with identities $e, f \in A$. Then $e = f$.*

Proof. We have $e = e * f$ because f is an identity. But $e * f = f$ because e is an identity. Thus $e = f$ (by transitivity of equality). □

Definition 5. Let $(A, *)$ be a magma with identity e.

Let $a, b \in A$. We say that b is an *inverse* of a with respect to $*$ if

$$a * b = b * a = e.$$

We say that a is *invertible* with respect to $*$ if a has and inverse in A with respect to $*$.

Proposition 2. *Let $(A, *)$ be an associative magma with identity e, and let $a, b, c \in A$ such that b and c are inverses of a with respect to $*$. Then $b = c$.*

Proof. Using associativity, we have

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

Thus $b = c$. □

1.3. **Submagmas.** Each of the types of algebraic objects we wish to study admit subobjects. Discussing this requires the notion of closure of a binary operation.

Definition 6. Let $(A, *)$ be a magma, and let $B \subset A$. We say that B is a *submagma* of A if

(C0) B is nonempty;
(C1) $b, c \in B \Rightarrow b * c \in B$.

Property **(C1)** is known as *closure*; we say that B is *closed under* $*$ if $b * c \in B$ whenever $b, c \in B$. This is exactly the property which makes $*$ (by restriction) a binary operation on B, so that $(B, *)$ is itself a magma.

Example 9. Let $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ denote the set of even integers. Then $2\mathbb{Z}$ is a submagma of $(\mathbb{Z}, +)$, as well as a submagma of $(\mathbb{Z}, \cdot)$.

Example 10. Let $B = \{\pm\vec{i}, \pm\vec{j}, \pm\vec{k}, \vec{0}\} \subset \mathbb{R}^3$ be the set of standard basis vectors and their negative in three dimensional space, together with the zero vector. Then B is closed under cross product, so B is a submagma of $(\mathbb{R}^3, \times)$.

1.4. **Notational Conventions.** Various conventions have developed over time regarding the notation surrounding binary operations, when they are used in a general setting. We list these conventions, and then we use them throughout.

Remark 1. If the operation is addition, the following conventions are in place:

(a) the operation is denoted by $+$;
(b) the identity element is denoted by 0;
(c) the inverse of a is denoted $-a$;
(d) if $n \in \mathbb{N}$, then na means $a + \cdots + a$, n times;
(e) if $n \in \mathbb{Z}$ is negative, then na means $n(-a)$.

Typically, addition is assumed to be commutative.

Remark 2. If the operation is multiplication, the following conventions are in place:

(a) the operation is denoted by $\cdot$, which is suppressed, so $a \cdot b$ is written ab;
(b) the identity element is denoted by 1;
(c) the inverse of a is denoted a^{-1};
(d) if $n \in \mathbb{N}$, then a^n means $a \cdot \cdots \cdot a$, n times;
(e) if $n \in \mathbb{Z}$ is negative, then a^n means $(a^{-1})^n$.

Remark 3. If we are discussing a specific magma, conventions for denoting the operation, inverses, "multiples" or "powers", and so forth, are already in place. However, we often wish to prove general results, where the magma involved is generic.

It has become traditional to denote the operation in a generic commutative magma using additive notation only if the operation is assumed to be commutative.

If it is unknown whether or not the operation is commutative, then multiplicative notation is used. Typically, even if the operation has another symbol, exponential notation is used for properties **(c)**, **(d)**, and **(e)** in the previous remarks. For example, composition ($\circ$) of functions uses exponential notation.

It is also traditional (and convenient) to indicate a magma by its underlying set; that is, we say "the magma M" to mean "the magma $(M, \cdot)$".

1.5. **Power Magmas.** A binary operation on a set induces a binary operation on the power set of the set, as follows.

Definition 7. Let $(A, *)$ be a magma. Let $b, c \in A$ and let $X, Y \subset A$. Define

(a) $b * X = \{b * x \mid x \in X\}$
(b) $X * b = \{x * b \mid x \in X\}$
(c) $X * Y = \{x * y \mid x \in X \text{ and } y \in Y\}$

Then **(c)** induces a binary operation, also denoted by $*$, on the power set $\mathcal{P}(A)$. We call $(\mathcal{P}(A), *)$ the *power magma* induced by $(A, *)$.

There are several observations we wish to make in this context.

- We point out that since A is closed under $*$, the sets $b * X$, $X * b$, and $X * Y$ are subsets of A. Thus, **(c)** implies that $*$ is closed on $\mathcal{P}(A)$, so $*$ is a binary operation on $\mathcal{P}(A)$. Thus $(\mathcal{P}(A), *)$ is a magma.
- If $(A, *)$ is associative, then for $b, c \in A$ and $X \subset A$, we have $(b * X) * c = b * (X * c)$, so we may write this simply as $b * X * c$.
- If e is an identity for $(A, *)$ and $e \in Y$, then $b \in b * Y$ and $X * Y \supset X$.
- If $(B, *)$ is a submagma of $(A, *)$, then $B * B \subset B$.
- If e is an identity for $(A, *)$ and $(B, *)$ is a submagma of $(A, *)$ containing e, then $B * B = B$.

In additive notation, our definition for setwise operations becomes

(a) $b + X = \{b + x \mid x \in X\}$
(b) $X + b = \{x + b \mid x \in X\}$
(c) $X + Y = \{x + y \mid x \in X \text{ and } y \in Y\}$

In multiplicative notation, our definition for setwise operations becomes

(a) $bX = \{bx \mid x \in X\}$
(b) $Xb = \{xb \mid x \in X\}$
(c) $XY = \{xy \mid x \in X \text{ and } y \in Y\}$

2. Monoids

Definition 8. A *monoid* $(M, *, e)$ consists of a set M together with a binary operation $*$ on M and an element $e \in M$ such that

(M1) $a * (b * c) = (a * b) * c$ for every $a, b, c \in A$;
(M2) $a * e = e * a = a$ for every $a \in A$.

That is, a monoid is an associative magma with identity.

Example 11. The natural numbers under addition or multiplication $(\mathbb{N}, +, 0)$ and $(\mathbb{N}, \cdot, 1)$ are monoids.

Example 12. Let X be a set and let X^ω be the set of all strings on X. Then X^ω is a monoid under the operation of concatenation. The identity element is the empty string.

Example 13. Let X be a set and let $\mathcal{F}(X) = \{f : X \to X\}$. Then $(\mathcal{F}(X), \circ, \mathrm{id}_X)$ is a monoid.

3. Groups

3.1. **Groups.** The most commonly discussed algebraic categories are groups, rings, and fields. Of the three, groups have the least structure (so there are more of them).

Definition 9. A *group* $(G, *, e)$ consists of a set G together with a binary operation $*$ on G and an element $e \in G$ such that

- **(G1)** $a * (b * c) = (a * b) * c$ for every $a, b, c \in A$;
- **(G2)** $a * e = e * a = a$ for every $a \in A$;
- **(G3)** for every $a \in G$ there exists $\widetilde{a} \in G$ such that $a * \widetilde{a} = \widetilde{a} * a = e$.

That is, a group is a monoid in which every element is invertible.

Example 14. The integers under addition $(\mathbb{Z}, +, 0)$ is a group. However, the multiplicative monoid $(\mathbb{Z}, \cdot, 1)$ is not a group, because the only invertible elements in $\mathbb{Z}$ (with respect to multiplication) are 1 and -1.

The rational numbers without zero form a multiplicative group $(\mathbb{Q}^*, \cdot, 1)$.

Example 15. Let n be a positive integer. Then $(\mathbb{Z}_n, +, \overline{0})$ and $(\mathbb{Z}_n^*, \cdot, \overline{1})$ are groups.

Example 16. Let X be a set. Then $(\mathcal{P}(X), \triangle, \varnothing)$ is a group. The inverse of $A \subset X$ is A, because $A \triangle A = \varnothing$.

Example 17. Let X be a set. Then $(\mathrm{Sym}(X), \circ, \mathrm{id}_X)$ is a group.

Example 18. Define the *general linear group* by

$$\mathbf{GL}_n(\mathbb{R}) = \{\text{invertible } n \times n \text{ matrices over} \mathbb{R}\}.$$

This is a group under matrix multiplication.

Definition 10. Let $(G, *, e)$ be a group. We say that G is *abelian* if

$$a * b = b * a \quad \text{for all } a, b \in G.$$

That is, an abelian group is a group whose operation is commutative.

Example 19. The numerical groups such as $(\mathbb{Z}, +, 0)$ and $(\mathbb{Z}_n^*, \cdot, \overline{1})$ are abelian, as is $(\mathcal{P}(X), \triangle, \varnothing)$. However, $(\mathrm{Sym}(X), \circ, \mathrm{id}_X)$ is not, nor are the matrix groups $\mathbf{GL}_n(\mathbb{R})$.

Remark 4. It is traditional (and convenient) to denote a group $(G, *, e)$ simply by G, where the operation $*$ is understood.

3.2. **Subgroups.** The subobjects in the category of groups are subsets which are themselves subgroups (with respect to the same binary operation).

Definition 11. Let $(G, *, e)$ be a group and let $H \subset G$. We say that H is a *subgroup* of G, and write $H \leq G$, if

- **(S0)** $e \in H$;
- **(S1)** $a, b \in H \Rightarrow a * b \in H$;
- **(S2)** $a \in H \Rightarrow \widetilde{a} \in H$.

These are exactly the conditions on a subset $H \subset G$ which guarantee that $(H, *, e)$ is itself a group. Condition **(S1)** is known as *closure*; if condition **(S1)** holds, we say that H is *closed under* $*$. In the case that H is nonempty and finite, this implies the other two conditions.

Example 20. Under addition, the standard number system form a chain of subgroups:

$$(\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0) \leq (\mathbb{R}, +, 0) \leq (\mathbb{C}, +, 0).$$

The even integers are a subgroup of $(\mathbb{Z}, +, 0)$.

Let $\mathbb{Z}^* = \{\pm 1\}$. Then $\mathbb{Z}^*$ is a subgroup of $\mathbb{Q}^*$ under multiplication; in fact,

$$(\mathbb{Z}^*, \cdot, 1) \leq (\mathbb{Q}^*, \cdot, 1) \leq (\mathbb{R}^*, \cdot, 1) \leq (\mathbb{C}, \cdot, 1).$$

Example 21. Define the *special linear group* by

$$\mathbf{SL}_n(\mathbb{R}) = \{A \in \mathbf{GL}_n(\mathbb{R}) \mid \det(A) = 1\}.$$

Then $\mathbf{SL}_n(\mathbb{R}) \leq \mathbf{GL}_n(\mathbb{R})$.

Proposition 3. *Let $(G, *, E)$ be a group and let $H \subset G$ be a finite nonempty subset satisfying*

$$a, b \in H \quad \Rightarrow \quad a * b \in H.$$

Then $H \leq G$.

Proof. We use exponential notation, so that $g^n = g * \cdots * g$, n times. In this context, g^0 is the identity, in this case e, and the inverse of h is h^{-1}.

Since H is nonempty, there exists an element $h \in H$. We wish to show that $e \in H$ and $h^{-1} \in H$.

Consider the set

$$K = \{h^n \mid n \text{ a positive integer}\}.$$

Since H is closed, $K \subset H$. Since H is finite, K is finite. Thus there exist distinct positive integers i and j such that $h^j = h^i$. We may assume that $i < j$.

Clearly, the inverse of h^n is h^{-n}, and $h^j * h^{-i} = h^{j-i}$. Then

$$h^j = h^i \Rightarrow h^j * h^{-i} = h^i * h^{-i} \Rightarrow h^{j-i} = h^{i-i} \Rightarrow h^{j-i} = e.$$

Let $k = j - i$; then $h^k = e$. Now $k > 0$; if $k = 1$, then $h = e$, and $e^{-1} = e$, so $h^{-1} \in H$. Otherwise, $k - 1 > 0$, so $h^{k-1} \in K \subset H$, and $h * h^{k-1} = e$; this implies that h^{k-1} is the inverse of h. Thus H satisfies **(S2)**. Moreover, by closure, $h * h^{-1} = e \in H$, proving **(S0)**. □

Henceforth, we will use multiplicative notation for a generic group.

3.3. **Cyclic Groups.** A group is *generated* by a set of elements if every element of the group can be written as a product of elements from the set, and their inverses. The simplest example of this occurs when there is a single generator.

Definition 12. Let G be a group, and let $g \in G$. The *subgroup generated by g* is

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

First we note that $\langle g \rangle$ is certainly a subgroup of G: it is a subset of G, because G is closed under the operation (written multiplicatively in this general case); it contains the identity 1, because $g^0 = 1$; it is closed, because $g^m g^n = g^{m+n}$; it contains inverses, because $(g^n)^{-1} = (g^{-1})^n$.

Definition 13. Let G be a group. We say that G is *cyclic* if there exists $g \in G$ such that $G = \langle g \rangle$.

Example 22. The group $(\mathbb{Z}_{10}^*, \cdot, \overline{1})$ is cyclic, since $\mathbb{Z}_{10}^* = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$, and if we let $g = \overline{3}$, we have $g^1 = \overline{3}$, $g^2 = \overline{9}$, $g^3 = \overline{27} = \overline{7}$, and $g^4 = \overline{81} = \overline{1}$.

The group $(\mathbb{Z}_{12}^*, \cdot, \overline{1})$ is not cyclic, since $\mathbb{Z}_{12}^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$, and $\overline{5}^2 = \overline{7}^2 = \overline{9}^2 = \overline{1}$.

Example 23. In additive notation, $\langle g \rangle$ consists of all integer multiples of g.

The group $(\mathbb{Z}, +, 0)$ is cyclic, because every element is a multiple of one. This remains true for $(\mathbb{Z}_n, +, \overline{0})$. In the first case, the group is infinite, and in the second, the group is finite. Note that in the finite case, we only need positive multiples to cover the entire group.

Definition 14. Let G be a group. The *order* of G is its cardinality, denoted $|G|$.

Let $g \in G$. The *order* of g, denoted $\text{ord}(g)$, is given by

$$\text{ord}(g) = \min\{n \in \mathbb{Z} \mid n > 0 \text{ and } g^n = 1\}.$$

Example 24. In $(\mathbb{Z}_{10}^*, \cdot, 1)$, we have computed that $\text{ord}(\overline{1}) = 1$, $\text{ord}(\overline{9}) = 2$, and $\text{ord}(\overline{3}) = \text{ord}(\overline{7}) = 4$.

In $(\mathbb{Z}_6, +, \overline{0})$, we use additive notation, and ask for the smallest multiple of an element that gives $\overline{0}$. We have $\text{ord}(\overline{0}) = 1$, $\text{ord}(\overline{3}) = 2$, $\text{ord}(\overline{2}) = \text{ord}(\overline{4}) = 3$, and $\text{ord}(\overline{1}) = \text{ord}(\overline{5}) = 6$.

It is clear that if $g \in G$, then $|\langle g \rangle| = \text{ord}(g)$. Thus G is cyclic if and only if there exists an element $g \in G$ with $|G| = \text{ord}(g)$. In this case, a generator for G is any element whose order is that of the group.

Proposition 4. *Let G be a group with $g \in G$, and let n be a positive integer. Then $g^n = 1$ if and only if $\text{ord}(g) \mid n$.*

Proof. Let $k = \text{ord}(g)$.

Suppose $g^n = 1$, and write $n = kq + r$, where $0 \leq r < k$. Then $g^{kq+r} = 1$, so $g^{kq}g^r = 1$, and since $g^{kq} = (g^k)^q = 1^q = q$, we have $g^r = 1$. Since k is the smallest positive integer such that $g^k = 1$, and $r < k$, it must be the case that r is not positive. Thus $r = 0$, so $n = kq$, and $k \mid n$.

Suppose that $k \mid n$. Then $n = kj$ for some $j \in \mathbb{Z}$, so $g^n = (g^k)^j = 1^j = 1$. □

3.4. **Cosets.** Cosets are "translations" of a subgroup.

Definition 15. Let G be a group and let $H \leq G$.

A *left coset* of H in G is a subset of G of the form

$$gH = \{k \in G \mid k = gh \text{ for some } h \in H\},$$

where $g \in G$. The *left coset space* of H in G is the set of all left cosets of H in G. This is denoted G/H. The *index* of H is G is $[G : H] = |G/H|$.

The next proposition characterizes when two elements of G produce the same coset.

Proposition 5. *Let G be a group and let $H \leq G$. Let $g_1, g_2 \in G$. Then*

$$g_1H = g_2H \quad \Leftrightarrow \quad g_1g_2^{-1} \in H.$$

Proof. Exercise. □

Note that in additive notation, a left coset looks like $g + H$.

Since $1 \in H$ and $g = g \cdot 1$, $g \in gH$. Thus, the union of the left cosets of H in G is G; that is, the cosets cover G, and every element of G is in some coset. We aim to show that each element of G is in *exactly* one coset, and moreover, all of the cosets have equal size. This will produce Lagrange's Theorem.

Proposition 6. *Let G be a group and let $H \leq G$. Let $g_1, g_2 \in G$. Then*

(a) *if $g_1H \cap g_2H$ is nonempty, then $g_1H = g_2H$.*

(b) *$|g_1H| = |g_2H|$;*

Proof. Suppose that $g_1H \cap g_2H$ is nonempty, and let $g \in g_1H \cap g_2H$. Then there exist $h_1, h_2 \in H$ such that $g = g_1h_1 = g_2h_2$. Thus $g_2^{-1}g_1 = h_2h_1^{-1}$, which is an element of H.

Let $g_3 \in g_1H$ so that $g_3 = g_1h_3$ for some $h_3 \in H$. Thus

$$g_3 = g_1h_3 = g_2g_2^{-1}g_1h_3 = g_2(h_2h_1^{-1}h_3);$$

since $h_2h_1^{-1}h_3 \in H$, this shows that $g_3 \in g_2H$. Similarly, if $g_4 \in g_2H$, then $g_4 \in g_1H$. Thus $g_1H = g_2H$, proving **(a)**.

Each element of g_1H can be written in a unique way as g_1h for some $h \in H$. Thus we may design a function $f : g_1H \to g_2H$ given by $g_1h \mapsto g_2h$. This function is clearly surjective. To see that it is injective, let $x_1, x_2 \in g_1H$ such that $f(x_1) = f(x_2)$. Now there exist $h_1, h_2 \in H$ such that $x_1 = g_1h_1$ and $x_2 = g_1h_2$. Thus $f(x_1) = g_2h_1$ and $f(x_2) = g_2h_2$, and these are equal, so $g_2h_1 = g_2h_2$. Multiplying on the left by g_2^{-1} gives $h_1 = h_2$, and multiplying again on the left by g_1 gives $g_1h_1 = g_1h_2$; that is, $x_1 = x_2$. Thus f is bijective. Since two sets have the same cardinality if and only if there exists a bijective function between them, this proves **(b)**. □

Proposition 7 (Lagrange's Theorem)**.** *Let G be a group and let $H \leq G$. Then*

$$|G| = |H|[G : H].$$

Proof. We have noted that every element in G is a coset; by Proposition 6 **(a)** each element of G is in a unique coset. Thus $|G|$ equals the sum of the cardinalities of these cosets. But by Proposition 6 **(b)**, each coset has the size cardinality, which is the cardinality of H. Thus $|G|$ equals the cardinality of H times the number of cosets of H in G. Thus $|G| = |H|[G : H]$. □

Proposition 8. *Let G be a group and let $g \in G$. Then* $\mathrm{ord}(g)$ *divides* $|G|$.

Proof. Let $H = \langle g \rangle$. By Lagrange's Theorem, $|G| = |H|[G : H] = \mathrm{ord}(g)[G : H]$. Thus $\mathrm{ord}(g)$ divides $|G|$. □

The following number theoretical propositions may be proved directly (in various different ways) from the division and euclidean algorithms, without reference to groups; however, the proof is very direct using Lagrange's Theorem.

Proposition 9 (Fermat's Little Theorem)**.** *Let p be a prime integer, and let $a \in \mathbb{Z}_p$. Then $a^p \equiv a \pmod{n}$.*

Proof. Consider the residue $\overline{a}$ of a in the group $\mathbb{Z}_p^*$. Since p is prime, every nonzero element in $\mathbb{Z}_p$ is invertible; therefore, the order of the group $\mathbb{Z}_p^*$ is $p - 1$. Thus $\overline{a}^{p-1} = 1$; multiplying both sides by $\overline{a}$ gives $\overline{a}^p = \overline{a}$. Therefore $a^p \equiv a \pmod{p}$. □

Definition 16. The *Euler phi function* is a function $\phi : \mathbb{N} \to \mathbb{N}$ given by

$$\phi(n) = \begin{cases} 0, \text{ if } n = 0 \text{ or } n = 1; \\ \text{the number of integers } a \text{ such that } 1 \leq a < n \text{ and } \gcd(a, n) = 1, \text{ if } n \geq 2. \end{cases}$$

So, for positive integers n, $\phi(n) = |\mathbb{Z}_n^*|$.

Proposition 10 (Euler's Theorem)**.** *Let n be a positive integer, and let $a \in \mathbb{Z}_n$ with $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Proof. Consider the residue $\overline{a}$ of a in the group $\mathbb{Z}_n^*$. The order of $\mathbb{Z}_n^*$ is $\phi(n)$, so $\overline{a}^n = 1$ in $\mathbb{Z}_n^*$. Therefore $a^{\phi(n)} \equiv 1 \pmod{n}$. □

3.5. **Normal Subgroups.** We would like to explore the conditions under which we can put the structure of a group on the left coset space G/H produced by a subgroup H of a group G. Note that our definition of left cosets is compatible with our earlier definition of setwise operations in power magmas.

We see that we may define right cosets $Hg = \{hg \mid h \in H$, As with left cosets, any two right cosets have the same cardinality, right cosets cover G, and distinct right cosets are disjoint.

Let G be a group and let $H \leq G$. Then G/H is the set of left cosets of H in G, and we may apply the setwise binary operations to the members of G/H. This produces a binary operation on G/H if and only if we always get another coset when we do this; that is, if

$$g_1H, g_2H \in G/H \quad \Rightarrow \quad \text{there exists } g_3 \in G \text{ such that } g_1Hg_2H = g_3H.$$

Note that $g_1g_2 \in g_1Hg_2H$, if g_1Hg_2H is a coset, it is the coset g_1g_2H. So, we wish to find a condition on H such that $g_1Hg_2H = g_1g_2H$ for all $g_1, g_2 \in G$.

Definition 17. Let G be a group and let $H \leq G$. We say that H is *normal* in G, and write $H \triangleleft G$, if

$$gH = Hg \quad \text{for all } g \in G.$$

That is, H is normal if its left and right cosets are equal. In an abelian group, we always have $gH = Hg$, so every subgroup of an abelian group is normal.

Proposition 11. *Let G be a group and let $H \triangleleft G$. Then G/H is a group under setwise multiplication.*

Proof. First we demonstrate that setwise multiplication is closed on G/H. Since H is closed, $HH \subset H$, but since $1 \in H$, $H \subset HH$. Thus $HH = H$.

Let $g_1, g_2 \in G$ so that g_1H and g_2H are arbitrary members of G/H. Since $H \triangleleft G$, $g_2H = Hg_2$; since the operation is associative, we have

$$(g_1H)(g_2H) = g_1(Hg_2)H = g_1(g_2H)H = (g_1g_2)(HH) = g_1g_2H.$$

So, the setwise product $(g_1H)(g_2H)$ is another coset, and we have a binary operation on G/H. Clearly, this operation inherits associativity from G. The identity element is $1 \cdot H = H$, because $(gH)H = gHH = gH$, and $HgH = gHH = gH$. The inverse of gH is $g^{-1}H$, because $(gH)(g^{-1}H) = g(Hg^{-1})H = (gg^{-1})(HH) = 1 \cdot H = H$. □

Definition 18. Let G be a group and let $H \triangleleft G$. We call G/H the *quotient group* of G modulo H.

4. Rings

4.1. **Rings.** Rings are set with two binary operations, typically (but not always) called addition and multiplication, which are related by the distributive law. We give the definition as in terms of addition and multiplication, but keep in mind that these may be changed, as long as the correspond properties which define a ring are left intact.

Definition 19. Let *ring* $(R, +, \cdot, 0, 1)$ consists of a set R, two binary operations $+$ and $\cdot$ on R, and two (not necessarily distinct) element $0, 1 \in R$, such that

(R1) $a + b = b + a$ for all $a, b \in R$;
(R2) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$;
(R3) $a + 0 = a$ for all $a \in R$;
(R4) for every $a \in R$ there exists $-a \in R$ such that $a + (-a) = 0$;
(R5) $a(bc) = (ab)c$ for all $a, b, c \in R$;
(R6) $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$:
(R7) $a(b + c) = ab + ac$ for all $a, b, c \in R$;
(R8) $(a + b)c = ac + bc$ for all $a, b, c \in R$.

That is, a ring is a set which is an abelian group under addition and a monoid under multiplication such that addition and multiplication are related by the distributive laws.

Example 25. Let $R = \{0\}$; there is only one way to define addition and multiplication, and if with let $1 = 0$, this becomes a ring, known as the *zero ring*.

Example 26. The standard numerical sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are rings under standard addition and multiplication.

Example 27. Let p be a positive prime integer, and set

$$\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{d} \in \mathbb{Q} \mid a, b \in \mathbb{Q}\}.$$

This is a ring; in fact, it is the smallest subring of $\mathbb{R}$ which contains $\sqrt{p}$.

Example 28. Consider $i \in \mathbb{C}$ and the set

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}.$$

This is a ring, known as the *ring of Gaussian integers*.

Example 29. Let n be a positive integer. Then $\mathbb{Z}_n$ is a ring.

Example 30. Let n be a positive integer and let $\mathcal{M}_{n\times n}(\mathbb{R})$ denote the set of square $n \times n$ matrices over $\mathbb{R}$. This is a ring under matrix addition and multiplication.

Example 31. Let X be a set and let $\mathcal{P}(X)$ be the power set of X. Then $(\mathcal{P}(X), \triangle, \cap, \varnothing, X)$ is a ring. The point here is that $\cap$ distributes over $\triangle$.

Proposition 12 (Cancellation Law of Addition)**.** *Let R be a ring and let $a, b, c \in R$. If $a + c = b + c$, then $a = b$.*

Proof. Add $-c$ to both sides. □

Proposition 13 (Multiplication by Zero)**.** *Let R be a ring and let $a \in R$. Then $a \cdot 0 = 0$.*

Proof. We have $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Thus $0 + a \cdot 0 = a \cdot 0 + a \cdot 0$, so by cancellation, $0 = a \cdot 0$. □

Proposition 14 (Multiplication by Negatives)**.** *Let R be a ring and let $a, b \in R$. Then $(-a)b = -(ab)$.*

Proof. Note what this is saying: if you take the additive inverse of a and multiply it by b, you get the additive inverse of the product ab.

Now since additive inverses are unique, it suffices to show that $(-a)b$ acts like an additive inverse of ab. This is true by the distributive property, since $ab + (-a)b = (a + (-a))b = 0 \cdot b = b \cdot 0 = 0$. □

Definition 20. Let R be a ring. We say that R is *commutative* if

(R9) $ab = ba$ for every $a, b \in R$.

Example 32. The standard numeric rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative. The ring $\mathcal{M}_{n\times n}(\mathbb{R})$ of $n \times n$ matrices over $\mathbb{R}$ is not commutative.

4.2. **Subrings.** Subobjects exist in the category of rings.

Definition 21. Let R be a ring, and let $S \subset R$. We say that S is a *subring* of R, and write $S \leq R$, if

(S0) $1 \in S$;
(S1) $a, b \in S \Rightarrow a + b \in S$;
(S2) $a \in S \Rightarrow -b \in S$;
(S3) $a, b \in S \Rightarrow ab \in S$.

These are the exact conditions that guarantee that S is a ring with respect to the same addition, multiplication, and identities. Note that if $S \leq R$, then $0 \in S$ because $1 \in S$ by **(S0)**, so $-1 \in S$ by **(S2)**, whence $1 + (-1) = 0 \in S$ by **(S1)**.

Example 33. The standard numeric rings form an increasing sequence of subrings $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$. Moreover, $\mathbb{Q}[\sqrt{5}]$ is a subring of $\mathbb{R}$, and $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ but not of $\mathbb{R}$.

Example 34. Let X be a set and let $Y \subset X$. Then $\mathcal{P}(Y) \leq \mathcal{P}(X)$.

Example 35. The set of upper triangular $n \times n$ matrices form a subring of the ring of all $n \times n$ matrices.

4.3. **Invertible and Entire Elements.** The cancellation law for multiplication holds only for some elements in a ring. For example, in $\mathbb{Z}_1 5$, $\overline{2} \cdot \overline{5} = \overline{8} \cdot \overline{5} = \overline{10}$, but $\overline{2} \neq \overline{5}$. We investigate this, working in a commutative ring; the definitions may be adjusted for the noncommutative case.

Definition 22. Let R be a commutative ring and let $a \in R$. We say that a is *invertible* if there exists $a^{-1} \in R$ such that $aa^{-1} = 1$. We call a^{-1} the *inverse* of a.

The invertible elements of $\mathbb{Z}$ are ± 1, and the invertible elements of $\mathbb{Z}_n$ are those $\overline{a} \in \mathbb{Z}_n$ such that $\gcd(a, n) = 1$.

Definition 23. Let R be a commutative ring and let $a \in R$.

We say that a is *entire* if

$$ab = 0 \quad \Rightarrow \quad b = 0, \qquad \text{for all } b \in R.$$

We say that a is a *zero-divisor* if $a \neq 0$ and there exists $b \in R$, $b \neq 0$, such that $ab = 0$.

Thus a is a zero divisor if and only if a is not entire and $a \neq 0$.

Proposition 15. *Let R be a commutative ring and let $a \in R$. If a is invertible, then a is entire.*

Proof. Suppose a is invertible, and that $ab = 0$. Multiply by a^{-1} to get $a^{-1}ab = a^{-1} \cdot 0$, so $b = 0$. □

Definition 24. Let R be a commutative ring and let $a \in R$. We say that a is *cancellable* if whenever $ab = ac$, then $b = c$.

Proposition 16. *Let R be a commutative ring and let $a \in R$. Then a is entire if and only if a is cancellable.*

Proof. Suppose that a is entire, and that $ab = ac$. Then $a(b - c) = 0$, and since a is entire, we have $b - c = 0$, whence $b = c$. Thus a is cancellable.

On the other hand, suppose a is cancellable, and that $ab = 0$. Then $ab = a \cdot 0$, so by the cancellability of a, $b = 0$. Thus a is entire. □

Definition 25. An *integral domain* is an commutative ring in which every element is entire.

Since every nonzero element of a field is invertible, every nonzero element of a field is entire, so a field is an integral domain. Thus $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are entire rings. Also, the ring of integers $\mathbb{Z}$ is an integral domain. We have seen that $\mathbb{Z}_n$ is entire if and only if it is a field, which happens if and only if n is prime.

4.4. **Irreducible and Prime Elements.** The standard definition for prime integer is actually not the correct general definition for prime element in a ring; they are equivalent, in the case of the integers, because of a result proved 2300 years ago in Euclid's *The Elements*.

Definition 26. Let R be a ring and let $p \in R$ be an entire noninvertible element.

We say that p is *irreducible* if whenever $p = ab$, then either a is invertible or b is invertible.

We say that p is *prime* if whenever $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proposition 17 (Euclid's Argument Part I)**.** *Let R be a ring and let $p \in R$. If a is prime, then a is irreducible.*

Proof. Suppose that p is prime, and suppose that $p = ab$. We wish to show that either a is invertible or b is invertible.

Since $p = ab$, we have $p \mid ab$, and since p is prime, either $p \mid a$ or $p \mid b$. Suppose that $p \mid a$; then $a = pc$ for some $c \in R$. Thus $p = pcb$, and since p is entire, it is cancellable, so $bc = 1$. Thus b is invertible.

Similarly, if $p \mid b$, then a is invertible. □

Proposition 18 (Euclid's Argument Part II)**.** *Let $p \in \mathbb{Z}$, $p \geq 2$. Then p is prime if and only if p is irreducible.*

Proof. We have just seen that in any ring, a prime element is irreducible.

Now assume that $p \in \mathbb{Z}$ is irreducible. Given that $a \mid p \Rightarrow a = 1$ or $a = p$, suppose that $p \mid ab$. Then there exists $k \in \mathbb{N}$ such that $kp = ab$. Suppose that p does not divide a; then $\gcd(a, p) = 1$. Thus there exist $x, y \in \mathbb{Z}$ such that $xa + yp = 1$. Multiply by b to get $xab + ypb = b$. Substitute kp for ab to get $(xk + yb)p = b$. Thus $p \mid b$. □

Notice that in the case $R = \mathbb{Z}$, our definition of irreducible is the same as Euclid's definition of prime. This is standard, and is allowable because, in the case of the integers, prime and irreducible are equivalent. This, however, is not the case in general. For example, consider the set $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. This is clearly a subring of $\mathbb{C}$. Let $z = 2 + \sqrt{-5}$, and notice that $3^2 = 9 = a\overline{a}$; now 3 is irreducible and divides 9, but it does not divide either of the factors a or $\overline{a}$.

It is the equivalence of primeness and irreducibility which leads to unique factorization in the integers. This equivalence comes from the Euclidean algorithm, which in turn comes from the division algorithm.

4.5. **Ideals.** If we "mod out" a group G by a normal subgroup H, the set of left cosets G/H is a group under the induced operation on the cosets, using setwise multiplication (or setwise addition, if the operation in G is addition). An ideal of a ring is analogous to a normal subgroup of a group; it is the ideal property **(I2)** that ensures that multiplication is well-defined on the cosets.

Definition 27. Let R be a commutative ring and let $I \subset R$ be nonempty. We say that I is an *ideal* of R, and write $I \lhd R$, if

(I1) $a, b \in I \Rightarrow a + b \in I$;
(I2) $a \in I$ and $x \in R \Rightarrow xa \in I$.

Proposition 19. *Let R be a commutative ring and let $I \lhd R$. Then I is an additive subgroup of $(R, +, 0)$.*

Proof. Since it is given by **(I1)** that I is closed under addition, we wish to show that I contains additive inverses. But this follows from **(I2)**, since $-1 \in R$, so for $a \in R$ we have $(-1)a = -a \in R$. □

Since I is an additive subgroup of R, it produces cosets; if $a \in R$, the coset in which it resides is denoted $a + I$. By Proposition 5, $a + I = b + I$ if and only if $a - b \in I$.

Proposition 20. *Let R be a commutative ring and let $I \lhd R$. Then R/I is a ring, under the induced operations*

$$(a + I) + (b + I) = (a + b) + I \quad \text{and} \quad (a + I)(b + I) = ab + I.$$

Proof. Since $(R, +, 0)$ is an abelian group under addition, the ideal I is a normal subgroup. Thus, R/I is a group under addition. We wish to use the ideal property to show that multiplication is well-defined.

Thus, suppose that $c \in a + I$ and $d \in b + I$. Multiplication is well-defined if $cd \in ab + I$, for in this case, $cd + I = ab + I$, and our definition of multiplication does not depend on the representatives we select for a coset.

Now $c \in a+I$ implies that $c-a \in I$, and $d \in b+I$ implies that $d-b \in I$. multiply the $c-a$ by d and apply **(I2)** to obtain $cd-ad \in I$; similarly, multiply $d-b$ by a to obtain $ad-ab \in I$. Since I is closed under addition, $(cd-ad)-(ad-ab) = cd-ab \in I$. Thus $cd \in ab + I$. □

4.6. **Quotient Rings.** The category of rings admits quotient objects, which are obtained by "modding out" a ring by an ideal.

Definition 28. Let R be a commutative ring and let $I \triangleleft R$. We call R/I the *quotient ring* of R modulo I.

Let $a, b \in R$. We say that a and b are *congruent modulo* I, and write $a \equiv b \pmod{I}$, if $a - b \in I$.

Note the 0 represents the zero element of R/I, which is $I = 0 + I$. So, an element of R represents the zero element of R/I if and only if it is in I. Moreover, if $a, b \in R$, then a and b represent the same member of R/I if and only if $a \equiv b \pmod{I}$; that is, if $a - b \in I$.

Definition 29. Let R be a commutative ring, and let $a \in R$. The *principal ideal* of R generated by a is

$$\langle a \rangle = aR = \{ar \mid r \in R\}.$$

It is easily verified that $aR \triangleleft R$.

Proposition 21. *Let R be a commutative ring and let $a \in R$. Then $aR \triangleleft R$.*

Proof. Exercise. □

Example 36. Consider the ring $\mathbb{Z}$, and let $n \in \mathbb{Z}$. Then $n\mathbb{Z} \triangleleft \mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ is a ring.

An interesting case of quotient rings is obtained by modding out by a principal ideal. If $a \in R$, an element of R represents the zero element of R/aR if and only if it is a multiple of a. As a consequence, R/aR is an integral domain if and only if a is prime.

Proposition 22. *Let R be a commutative ring and let $a \in R$. Then R/aR is an integral domain if and only if a is prime.*

Proof. Exercise. □

It is often convenient to let $\langle a \rangle$ denote the smallest ideal in R which contains a; this is aR. That is,

$$\langle a \rangle = aR.$$

5. Fields

5.1. **Fields.** Fields are ring in which division is possible.

Definition 30. A *field* is a commutative ring F such that

(R10) for every $a \in F$ there exists $a^{-1} \in F$ such that $aa^{-1} = a^{-1}a = 1$.

Noting that every ring has an underlying structure of an additive abelian group, we now have the following hierarchy:

- Set + binary operation = Magma
- Magma + associativity + identity = Monoid
- Monoid + invertibility = Group
- Group + commutativity = Abelian Group
- Additive Group + associative multiplication with id + distribution = Ring
- Ring + commutativity of multiplication = Commutative Ring
- Commutative Ring + entireness = Integral Domain
- Integral Domain + multiplicative invertibility = Field
- Field

Example 37. These are fields: $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. These are not fields: $\mathbb{N}$, $\mathbb{Z}$.

Example 38. Let

$$\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}.$$

Then $\mathbb{Q}[\sqrt{5}]$ is a field: we compute the inverse of $a + b\sqrt{5}$ as follows:

$$\frac{1}{a + b\sqrt{5}} = \frac{a - b\sqrt{5}}{(a + b\sqrt{5})(a - b\sqrt{5})} = \frac{a - b\sqrt{5}}{a^2 - 5b^2} = \frac{a}{a^2 - 5b^2} + \frac{-b}{a^2 - 5b^2}\sqrt{5} \in \mathbb{Q}[\sqrt{5}].$$

Example 39. The ring $\mathbb{Z}_n$ is a field if and only if n is prime.

Note that every nonzero element of a field is entire, because it is invertible.

5.2. **Subfields.** Of course, subobjects exists in the category of fields.

Definition 31. Let E be a field and let $F \subset E$. We say that F is a *subfield* of E, and write $F \leq E$, if

(S0) $1 \in F$;
(S1) $a, b \in F \Rightarrow a + b \in F$;
(S2) $a \in F \Rightarrow -b \in F$;
(S3) $a, b \in F \Rightarrow ab \in F$;
(S4) $a \in F \setminus \{0\} \Rightarrow a^{-1} \in F$.

Example 40. We have $\mathbb{Q} \leq \mathbb{Q}[\sqrt{5}] \leq \mathbb{R} \leq \mathbb{C}$.

We required polynomials to produce more examples of fields, and to more fully develop their theory.

6. Polynomials

6.1. **Polynomials.** We like to think of polynomials as functions, but in the case where the coefficients come from finite fields, it is more powerful to make the following definition.

Definition 32. Let R be a commutative ring. A *polynomial over* R is a formal sum

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

where $a_i \in R$ for $i = 0, \ldots, n$. It is the *zero polynomial* if $n = 0$ and $a_n = 0$; otherwise assume that $a_n \neq 0$. The numbers a_i are called the *coefficients* of f.

We call n the *degree* of f, denoted $\deg(f)$. We call a_n the *leading coefficient* of f, denoted $\mathrm{LC}(f)$. We call a_0 the *constant coefficient* of f, denoted $\mathrm{CC}(f)$. We say that f is *monic* if $a_n = 1$.

The set of all polynomials over R is denoted $R[x]$.

We identify a constant polynomial of the form $f(x) = a_0$ with the element $a_0 \in R$; in this way, we view R as a subring of $R[x]$.

By convention, the expression $0x^k$ is defined to be $0 \in R$.

Definition 33. We give names to polynomials based on their degrees, as follows:

- A *constant* polynomial is a polynomial of degree 0.
- A *linear* polynomial is a polynomial of degree 1.
- A *quadratic* polynomial is a polynomial of degree 2.
- A *cubic* polynomial is a polynomial of degree 3.
- A *quartic* polynomial is a polynomial of degree 4.
- A *quintic* polynomial is a polynomial of degree 5.

Definition 34. Let R be a commutative ring and let $f, g \in R[x]$. Let $m = \deg(f)$ and $n = \deg(g)$. Write

$$f(x) = \sum_{i=0}^{m} a_i x^i \quad \text{and } g(x) = \sum_{i=0}^{n} b_i x^i.$$

If $k > m$, set $a_k = 0$, and if $k > n$, set $b_k = 0$. Define the *sum* and *product* of f and g by

$$(f+g)(x) = \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) x^i,$$

and

$$(fg)(x) = \sum_{i=0}^{m+n} \Big(\sum_{k=0}^{i} a_k b_{i-k} \Big) x^i.$$

This produces the operations of addition and multiplication of polynomials on the set $R[x]$.

Note that the definitions of the sum and product of polynomials are constructed so that addition and multiplication of polynomials is accomplished in the way we are accustomed; distribute and combine like terms.

Proposition 23. *Let R be a commutative ring. Then $R[x]$ is a commutative ring.*

Reason. We defined addition and multiplication so that properties **(R1)** through **(R9)** are preserved. □

We will typically consider the ring of polynomials over an integral domain or, even better, a field. Actually, since integers are rational numbers, we view $\mathbb{Z}[x]$ as a subring of $\mathbb{Q}[x]$.

If R is not entire, we can run into problems with standard properties of polynomials in $R[x]$ which we want, as indicated in the next proposition.

Proposition 24. *Let R be an entire commutative ring and let $f, g \in R[x]$. Then*

(a) $\deg(f+g) = \max\{\deg(f), \deg(g)\}$, *unless* $\mathrm{LC}(f) - \mathrm{LC}(g) = 0$.

(b) $\deg(fg) = \deg(f) + \deg(g)$, *unless* $\mathrm{LC}(f)\mathrm{LC}(g) = 0$.

We give an example where the condition of entireness of the leading coefficients is important. Let $R = \mathbb{Z}_6$, $f(x) = 2x^3 + x^2 + 5$, and $g(x) = 3x^2 + 5x + 3$. Then, computing in $\mathbb{Z}_6[x]$, we have

$$(fg)(x) = \overline{6}x^5 + \overline{10+3}x^4 + \overline{6+5}x^3 + \overline{3+15}x^2 + \overline{25}x + \overline{3} = x^4 + 5x^3 + x + 3.$$

6.2. **The Division Algorithm for Polynomials.** Henceforth, let F be a field and let $F[x]$ be the ring of polynomials over F. In this case, we can divide by the leading coefficients and obtain an inductive process that allows polynomial division; this produces a strong analogy between integer arithmetic and polynomial arithmetic, which we now develop.

Proposition 25 (Division Algorithm for Polynomials)**.** *Let $f, g \in F[x]$, where f and g are nonzero. Then there exist polynomials $q, r \in F[x]$ such that*

$$g = fq + r, \qquad \textit{where} \qquad \deg(r) < \deg(f).$$

We call q the quotient *and r the* remainder.

Proof. If $\deg(f) > \deg(g)$, let $q = 0$ and $r = g$. Otherwise, we have $\deg(f) \leq \deg(g)$.

We write the proof to mimic the well-known algorithm for division; we proceed by strong induction on the larger degree $\deg(g)$.

If $\deg(f) > \deg(g)$, let $q = 0$ and $r = g$. Otherwise, we have $\deg(f) \leq \deg(g)$.

Let $d = \deg(g) - \deg(f)$; then $d \geq 0$. Since f is nonzero, $\mathrm{LC}(f) \neq 0$; set $a = \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)}$. Then $a \in F$, and the highest order term of $g(x)$ is f times ax^d.

Let $q_1 = g - fax^d$; then $q_1 \in F[x]$, and $\deg(q_1) < \deg(g)$. By induction on the degree, there exist polynomials q_2, r such that $q_1 = fq_2 + r$, with $\deg(r) < \deg(f)$. Thus $fq_2 + r = g - fax^d$. With $q = q_2 + ax^d$, we have $g = fq + r$. □

Proposition 26 (Remainder Theorem)**.** *Let $g \in F[x]$ and let $a, r \in F$. Define $f \in F[x]$ by $f(x) = x - a$. and let $g = fq + r$ where $\deg(r) < \deg(f)$. Then $r \in F$, and $f(a) = r$.*

Proof. Since $\deg(f) = 1$ and $\deg(r) < \deg(f)$, we must have $\deg(r) = 0$, so $r \in F$. Now $g(a) = f(a)q(a) + r = (a - a)q(a) + r = r$. □

Definition 35. Let $f, g \in F[x]$. We say that f *divides* g, and write $f \mid g$, if there exists $q \in F[x]$ such that $g = fq$.

The following are synonyms: f divides g, f is a factor of g, g is a multiple of f.

Proposition 27 (Factor Theorem)**.** *Let $g \in F[x]$ and let $a \in F$. Define $f \in F[x]$ by $f(x) = x - a$. Then*

$$f \mid g \quad \Leftrightarrow \quad g(a) = 0.$$

Proof. If $f \mid g$, then $g = fq$ for some $q \in F[x]$, and $g(a) = (a-a)q(a) = 0$.

On the other hand, if $g(a) = 0$, we divide g by f to obtain $g = fq + r$ with $\deg(r) < \deg(f)$. By the Remainder Theorem, $g(a) = r = 0$, so $g = fq$, and $f \mid g$. □

Definition 36. Let $f \in F[x]$ and $a \in F$. We say that a is a *root* of f if $f(a) = 0$.

Proposition 28 (Bound on Roots Corollary)**.** *Let $g \in F[x]$. Then the number of roots of g cannot exceed* $\deg(g)$.

Proof. Let $n = \deg(f)$, and let $a \in F$ is a root and set $f(x) = x - a$. Then $g = fq$ for some q, where $\deg(q) = n - 1$. By induction, q has at most $n - 1$ roots, and these together with a make at most n roots for f. □

6.3. **The Euclidean Algorithm.** An analog of the Euclidean algorithm for integers exists for polynomials.

Definition 37. Let $f, g \in F[x]$. A *greatest common divisor* of f and g is a polynomial $d \in F[x]$ satisfying

(a) $d \mid f$ and $d \mid g$;
(b) $e \mid f$ and $e \mid g$ implies $e \mid d$, for any $e \in F[x]$.

Proposition 29. *Let $f, g \in F[x]$. If $f \mid g$ and $g \mid f$, then $g = af$ for some $a \in F$.*

Proof. If $f \mid g$ and $g \mid f$, then $g = hf$ and $f = kg$ for some $h, k \in F[x]$. Then $g = hkg$, so $\deg(g) = \deg(hk) + \deg(g)$, so $\deg(hk) = 0$, and $hk \in F$. Set $a = hk$. □

Proposition 30. *Let $f, g, d, e \in F[x]$. If d and e are greatest common divisors of f and g, then $d = ae$ for some $a \in F$. Thus there is a unique monic greatest common divisor, which we denote by* $\gcd(f, g)$.

Proof. Suppose d and e are greatest common divisors of f and g. By **(b)** of the definition, $e \mid d$ and $d \mid e$. Thus $d = ae$ for some $a \in F$. Divide any greatest common divisor by its leading coefficient to obtain the unique monic greatest common divisor. □

Lemma 1. *Let $g, f, q, r \in F[x]$ with $g = fq + r$ and $\deg(r) < \deg(f)$. Then* $\gcd(g, f) = \gcd(f, r)$.

Proof. Let $d = \gcd(g, f)$; we wish to show that $d = \gcd(f, r)$.

Now $r = g - fq$, and d divides g and f; this means that $g = dq_1$ and $f = dq_2$ for some $q_1, q_2 \in F[x]$. Thus $r = d(q_1 - q_2)$, and $d \mid r$; **(a)** is satisfied.

Suppose that $e \mid f$ and $e \mid r$ for some $e \in F[x]$. Then $f = eq_3$ and $r = eq_4$ for some $q_3, q_4 \in F[x]$. Then $g = fq + r = eq_3q + eq_4 = e(q_3q + q_4)$. Thus $e \mid g$. Since $d = \gcd(g, f)$, $e \mid d$; **(b)** is satisfied. □

Proposition 31 (Euclidean Algorithm for Polynomials)**.** *Let $f, g \in F[x]$. Then $d = \gcd(f, g)$ exists, and there exist polynomials $s, t \in F[x]$ such that*

$$fs + gt = d.$$

Proof. Without loss of generality, we may assume that $\deg(g) \geq \deg(f)$; we proceed by induction on the smaller degree $\deg(f)$.

By the division algorithm, there exist $q, r \in F[x]$ such that $g = fq + r$, and $\deg(r) < \deg(f)$. By induction, there exist polynomials $s_1, t_1, d \in F[x]$ such that $d = \gcd(f, r)$ and $rs_1 + ft_1 = d$. Since $r = g - fq$, we have $(g - fq)s_1 + ft_1 = d$. Set $s = t_1 - q$ and $t = s_1$ to obtain $fs + gt = d$. Moreover, $d = \gcd(g, f)$ by the lemma. □

Example 41. Let $F = \mathbb{Z}_5$ with $f, g \in F[x]$ given by $f(x) = x^3 + 3$ and $g(x) = x^4 + x^3 + x^2 + 3$. Find $d = \gcd(f, g)$, and find $s, t \in F[x]$ such that $fs + gt = d$.

Solution. Using polynomial division, we begin by dividing f into g, then the remainder r into f, and so forth, until we obtain a zero remainder:

$$\begin{aligned} x^4 + x^3 + x^2 + 3 &= (x^3 + 3)(x + 1) + (x^2 + 2x) \\ x^3 + 3 &= (x^2 + 2x)(x + 3) + (4x + 3) \\ x^2 + 2x &= (4x + 3)(4x) + 0 \end{aligned}$$

The last nonzero remainder is a greatest common divisor. To make it monic, divide by four. The inverse of 4 in $\mathbb{Z}_5$ is 4, and $4(4x + 3) = x + 2$. Thus $\gcd(f, g) = x + 2$. Now unwind these equations, as we have before for integers:

$$\begin{aligned} 4(x + 2) &= (x^3 + 3) - (x^2 + 2x)(x + 3) \\ &= f(x) - [g(x) - f(x)(x + 1)](x + 3) \\ &= f(x)(1 + (x + 1)(x + 3)) - g(x)(x + 3) \\ &= f(x)(x^2 + 4x + 4) + g(x)(4x + 2) \end{aligned}$$

Thus

$$x + 2 = f(x)(4x^2 + x + 1) + g(x)(x + 3).$$

We have $s(x) = 4x^2 + x + 1$ and $t(x) = x + 3$. □

6.4. **Irreducibility.** The concepts of prime and irreducible elements are defined in any ring; we have seen that in the case of the ring of integers, these concepts are equivalent. The proof there relied on the Euclidean algorithm, so it is no surprise that prime and irreducible are also equivalent in the ring of polynomials over a field.

Definition 38. Let $f \in F[x]$ be nonconstant. We say that f is *reducible over* F if there exist $g, h \in F[x]$, with $\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$, such that $f = gh$. Otherwise, we say that f is *irreducible*.

Note that if $f \in F[x]$ is nonzero and $a \in F$, we can always let $g = af$ and $h = \frac{1}{a}f$ to get $f = gh$. This is referred to as an improper factorization. We are not interested in these. Thus, f is irreducible if

$$f = gh \Rightarrow g \in F \text{ or } h \in F.$$

What we call irreducible here is the analog of what was called prime by Euclid in the case of the integers.

Proposition 32 (Euler's Argument for Polynomials)**.** *Let $f, g, h \in F[x]$ be nonzero with f irreducible, and suppose that $f \mid gh$.*
Then $f \mid g$ or $f \mid h$.

Proof. Suppose that f does not divide g; we show that f divides h.

Since f is irreducible, the only factors of f are constants and constant multiples of f. Since f does not divide g, the only common factors are constants. Thus $\gcd(f, g) = 1$, and there exist polynomials $s, t \in F[x]$ such that

$$fs + gt = 1.$$

Multiplying this equation by h gives $fhs + ght = h$. Since f divides gh, we have $gh = fk$ for some $k \in F[x]$. Thus $fhs + fkt = h$, so $f(hs + kt) = h$, whence f divides h. □

Proposition 33 (Fundamental Theorem of Polynomial Arithmetic)**.** *Let $f \in F[x]$. Then there exist irreducible polynomials $p_1, \ldots, p_r \in F[x]$, unique up to order and multiplication by constants, such that $f = \prod_{i=1}^{r} p_i$.*

Proof. If f is irreducible, set $r = 1$ and $p_1 = f$. Otherwise, f has a proper factorization $f = gh$ where $\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$. By induction on the degree, we declare that g and h are products of irreducible elements, and so then if f.

Uniqueness follows from Euclid's argument. Thus suppose that $f = p_1 \cdots p_r = q_1 \cdots q_s$ for some positive integers r, s and irreducible polynomials p_i, q_j. Then p_1 divides $q_1 \ldots q_s$, so by repeated use of Euclid's argument, p_1 divides one of the q_j's; without loss of generality, we may assume that p_1 divides q_1. Since q_1 is irreducible and p_1 is nonconstant, we must have $q_1 = ap_1$ for some $a \in F$. Factoring out q_1 and continuing this process, we see that the each of the q_j's is a constant multiple of one of the p_i's, and that $r = s$. □

6.5. **Quotients of Polynomial Rings.** Let F be a field and let $R = F[x]$. Let $\langle f \rangle = fR$ denote the principal ideal generated by f in R. A polynomial from $F[x]$ is in $\langle f \rangle$ if and only if it is a multiple of f by another polynomial.

Consider the factor ring $\overline{R} = R/\langle f \rangle$. For $g \in R$, let $\overline{g} = g + \langle f \rangle$. We know that $\overline{g+h} = \overline{g} + \overline{h}$ and $\overline{gh} = \overline{g}\overline{h}$. We also know that $\overline{g} = \overline{h}$ if and only if $g - h \in \langle f \rangle$, that is, if $f \mid g - h$. In particular, $\overline{f} = \overline{0}$.

Let $g \in R$, and divide g by f to get

$$g = fq + r \quad \text{where } \deg(r) < \deg(f).$$

Thus, in $\overline{R}$, we have

$$\overline{g} = \overline{f}\overline{q} + \overline{r} = \overline{0}\overline{q} + \overline{r} = \overline{r}.$$

In this way, every member of $\overline{R}$ is represented by a polynomial of degree less than f. Suppose that $r_1, r_2 \in R$ with $\overline{r_1} = \overline{r_2}$, $\deg(r_1) < \deg(f)$ and $\deg(r_2) < \deg(f)$. Then $r_1 - r_2 \in I$; but every nonzero polynomial in I has degree at least $\deg(f)$, but $\deg(r_1 - r_2) < \deg(f)$. Thus $r_1 - r_2 = 0$, so $r_1 = r_2$. We have shown the following.

Proposition 34. *Let F be a field and $f \in F[x]$. Then every member of $F[x]/fF[x]$ is represented by a unique polynomial of degree less than* $\deg(f)$.

That is, there is a bijective correspondence between the set of polynomials in $F[x]$ of degree less than $\deg(f)$, and the members of $F[x]/\langle f \rangle$. We compute in $F[x]/\langle f \rangle$ by using the relation $\overline{f} = 0$.

Example 42. Let $F = \mathbb{Z}_5$ and $f = x^2 + x + 1$; we consider $F[x]/\langle f \rangle$. We have $\overline{f} = 0$, so $\overline{x^2} = \overline{-(x+1)} = \overline{4x+4}$. If $g(x) = x + 2$ and $h(x) = x + 3$; then $gh(x) = x^2 + 5x + 6 = x^2 + 1$. Thus $\overline{gh} = \overline{x^2+1} = \overline{4x+4+1} = \overline{4x}$.

7. Finite Fields

We construct finite fields as the quotient rings of polynomial ring modulo the ideal of an irreducible polynomial.

Proposition 35. *Let F be a field, and let $f \in F[x]$ be an irreducible polynomial over F. Then $F[x]/\langle f \rangle$ is a field.*

Proof. It suffices to show that every element of $F[x]/\langle f \rangle$ is invertible.

Thus let $g \in F[x]$, and let $\overline{g} = g + \langle f \rangle$. By the division algorithm, there exist $q, r \in F[x]$ such that $g = fq + r$, where $\deg(r) < \deg(f)$. Now $\overline{g} = \overline{fq + r} = \overline{f}\overline{q} + \overline{r} = \overline{r}$, because $\overline{f} = \overline{0}$. Thus, we may assume that $\deg(g) < \deg(f)$.

Since f is irreducible and $\deg(g) < \deg(f)$, $\gcd(f, g) = 1$, so there exist $s, t \in F[x]$ such that $fs + gt = 1$. In $F[x]/\langle f \rangle$, we have

$$\overline{1} = \overline{fs + gt} = \overline{f}\overline{s} + \overline{g}\overline{t} = \overline{g}\overline{t}.$$

Thus, $\overline{g}$ is invertible, with inverse $\overline{t}$. □

Let $\mathbb{F}_p = \mathbb{Z}_p$; this is the unique finite field containing p elements. To obtain additional finite fields, we select a polynomial $f \in \mathbb{F}_p[x]$ which is irreducible, and "mod out" by the ideal generated by f.

Proposition 36. *Let p be a positive prime integer and let $f \in \mathbb{F}_p[x]$ be irreducible, with $\deg(f) = r$. Then $F[x]/\langle f \rangle$ is a finite field containing p^r elements.*

Proof. There is a bijective correspondence between elements of $\mathbb{F}_p[x]/\langle f \rangle$ and polynomials in $\mathbb{F}[x]$ whose degree is less than r; each polynomial of degree less then r represents a unique coset of $\langle f \rangle$ in $\mathbb{F}_p[x]$. Each such polynomial is determined by a choice of coefficients $a_0, \ldots, a_{r-1}$. There are p choices for each a_i, so altogether there are p^r such polynomials. □

It can be shown that, up to equivalence of structure, there is a unique finite field containing q elements if $q = p^r$ for some prime p and power r. This field is denoted $\mathbb{F}_q$.

Example 43. Let $F = \mathbb{F}_2 = \{0, 1\}$. The polynomial $f(x) = x^2+x+1$ is irreducible over $\mathbb{F}_2$; let $E = \mathbb{F}_2[x]/\langle f\rangle$. Let $\alpha = x + \langle f\rangle$, the coset of $\langle f\rangle$ in $\mathbb{F}_2[x]$ containing x. Then $E = \{0, 1, \alpha, \alpha + 1\}$. The addition table for the field E is

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

It isn't hard to see where this comes from: any multiple of 2 is zero in this ring, so $\alpha + \alpha = 0$.

The multiplication table is

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

To compute this, we use the fact that $x^2 + x + 1 \in \langle f\rangle$, and $\langle f\rangle$ is the zero element in this ring. So, $\alpha^2 + \alpha + 1 = 0$, so $\alpha^2 = -\alpha - 1 = \alpha + 1$ (since $1 = -1$ in this ring).

8. Exercises

Problem 1. Let G be a group such that $g^2 = 1$ for every $g \in G$. Show that G is abelian.

Problem 2. Let G be a group with $H, K \leq G$. Show that $H \cap K \leq G$.

Problem 3. Let G be a group with $H \leq G$ and $K \leq H$ Show that

$$[G : K] = [G : H][H : K].$$

Problem 4. Let G be a group and let $H \triangleleft G$. Let $g \in G$ of finite order and let $\overline{g} = gH \in G/H$. Show that $\mathrm{ord}(\overline{g})$ divides $\mathrm{ord}(g)$.

Problem 5. Let G be a group and let $H \triangleleft G$. Suppose $|G| = 180$ and $|H| = 30$. Show that if G has an element of order 5, it is in H.

Problem 6. Let G be a group such that $g^2 = 1$ for every $g \in G$. Show that G is abelian.

Problem 7. Find an element of $\mathbb{Z}_7$ which reasonably interprets the expression.

(a) $1/2$
(b) $-2/3$
(c) $\sqrt{-3}$

Problem 8. Find all elements in $\mathbb{Z}_7$ which are solutions to the equation.

(a) $x^2 - 1 = 0$
(b) $x^3 - 1 = 0$
(c) $x^6 - 1 = 0$
(d) $x^3 - 5x + 4 = 0$

Definition 39. Let R be a ring and let $a \in R$.

We say that a is *idempotent* if $a^2 = a$.

We say that a is *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$.

Problem 9. Let R be a commutative ring, and let $a \in R$ be idempotent. Show that $2a = 0$.

Problem 10. Let R be a ring in which every element is idempotent. Show that R is commutative.

Problem 11. Let R be a ring and let $a \in R$ be idempotent. Show that aR is a monoid under multiplication with identity a.

Problem 12. Let R be a ring and let $M = \{a \in R \mid a \text{ is idempotent}\}$. Show that M is a monoid under multiplication.

Problem 13. Let R be a ring and let $M = \{a \in R \mid a \text{ is nilpotent}\}$. Show that M is a monoid under multiplication.

Problem 14. Let R be a ring and let $M = \{a \in R \mid a \text{ is entire}\}$. Show that M is a monoid under multiplication.

Problem 15. Let F be a finite field of cardinality q, and suppose that $q \equiv 3 \mod 4$.
Show that the polynomial $f(X) = X^2 + 1$ is irreducible over F.

Problem 16. Let $\mathbb{Q}[\sqrt{5}]$ denote the subset of the field $\mathbb{R}$ given by

$$\mathbb{Q}[\sqrt{5}] = \{x + y\sqrt{5} \mid x, y \in \mathbb{Q}\}.$$

Show that $\mathbb{Q}[\sqrt{5}]$ is a subfield of $\mathbb{R}$.

Department of Mathematics and CSci, Southern Arkansas University
E-mail address: plbailey@saumag.edu