Lecture Notes, Week 2

Math 480A2: Mathematics of Blockchain Protocols, Fall 2022

Lecturer: Bryan Gillespie

Commutative Rings and Fields

Due to the requirement of practical cryptography to work on real-world computers, cryptographic tools make use of mathematical objects which can be represented using a finite and controlled amount of information. This leads to the use of *finite fields* (also called *Galois fields*), and discrete objects defined over them, as the fundamental mathematical constructions used in cryptographic protocols. Over the next several weeks, we will study the algebraic background required to construct and classify the finite fields, and to understand their relation with polynomial rings.

Definition 1. A **ring** R is a set equipped with an addition operation $(+)$ and a multiplication operation $(\cdot)$ such that

- $(R, +)$ is an abelian group with identity element written "0"
- $(R, \cdot)$ is a monoid, meaning it is associative and has an identity element, written "1"
- Multiplication is distributive over addition

A ring is called a **commutative ring** if its multiplication operation is commutative.

Exercise 2. Write out the axioms of a ring R explicitly.

We will work primarily in the context of commutative rings.

Definition 3. Let R be a nonzero commutative ring. An element $a \in R$ is called a **unit** if there exists a nonzero element $b \in R$ such that $a \cdot b = 1$, or in other words, if a has a multiplicative inverse. The ring R is called a **field** if every nonzero element is a unit.

Example 4. The following sets with their usual arithmetic operations are commutative rings:

- The standard sets of numbers $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.
- The polynomials $R[x]$, where R is a commutative ring.
- The integers modulo a natural number, $\mathbb{Z}/n\mathbb{Z}$.

In addition, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}/p\mathbb{Z}$ (for p a prime) are fields.

Definition 5. Let R and R' be commutative rings. A function $\varphi : R \to R'$ is called a **homomorphism** if for $a, b \in R$, $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, and $\varphi(1_R) = 1_{R'}$. If φ maps R to itself then it is called an **endomorphism**, and if φ is bijective then it is called an **isomorphism**.

Remark 6. Homomorphisms can be thought of as "functions which preserve arithmetic". If R and R' are commutative rings for which there exists an isomorphism $\varphi : R \to R'$, then R and R' can be considered "equivalent" up to relabeling of elements, in the sense that φ provides a relabeling rule for the elements of R which preserves the arithmetic operations of the rings.

Definition 7. Let R be a commutative ring. An **ideal** of R is a nonempty subset I which is closed under addition with elements in I, and under multiplication with elements in R.

Remark 8. Every nonzero commutative ring R has at least two distinct ideals, the **zero ideal** $\{0\}$ and the **unit ideal** R. These are the only two ideals of R exactly when R is a field.

Several additional operations are useful for constructing new ideals from existing ones.

Proposition 9. *If I, J are ideals of a commutative ring R, then the following sets are also ideals:*

- *$I + J$, the set of elements $\{a + b : a \in I, b \in J\}$*
- *$I \cap J$*
- *$I \cdot J$, the set of finite R-linear combinations of elements in $\{a \cdot b : a \in I, b \in J\}$*

Proposition 10. *Let R be a commutative ring, and let $A \subseteq R$. Then the set of all finite R-linear combinations of elements in A,*

$$(A) \coloneqq \{r_1 a_1 + \ldots + r_k a_k : k \in \mathbb{N}, r_1, \ldots, r_k \in R, a_1, \ldots, a_k \in A\}$$

is an ideal of R.

The ideal described above is called the ideal *generated* by the finite set A. If $A = \{a_1, \ldots, a_n\}$ is a finite set, then sometimes the ideal generated by A is instead written $(a_1, \ldots, a_n)$. The term "unit ideal" for the underlying ring R is because $(u) = R$ for any unit $u \in R$ (and moreover, any ideal containing a unit is equal to R).

The following construction is fundamental to much of the upcoming theory.

Proposition 11. *Let R be a commutative ring, and let $I \subseteq R$ be an ideal. Then the collection of additive cosets $R/I \coloneqq \{a + I : a \in R\}$ form a commutative ring under the addition and multiplication rules*

- *$(a + I) + (b + I) = (a + b) + I$, and*
- *$(a + I) \cdot (b + I) = (a \cdot b) + I$.*

These rules are well-defined with respect to the choice of coset representatives, and the commutative ring is called the ***quotient ring*** *of R by I.*

Remark 12. The formalism of the above construction belies a simpler interpretation: the quotient ring of R by I is the ring obtained from R by interpreting the elements of I as "equivalent to zero". If I is the ideal generated by some elements, then these elements are sometimes called new **relations** for the quotient ring. For instance, in $\mathbb{Z}/5\mathbb{Z}$, the ideal $5\mathbb{Z}$ of integers divisible by 5 represents the standard integers which are "equal to 0" in the new quotient. Thus it is fine in this ring to think of the number 12 as $2 + 2 \cdot 5$, and since 5 is set to zero in the quotient ring, it's okay to ignore it and think of 12 as 2 instead. The formal definition of a quotient ring means that this interpretation is fine, and nothing goes wrong with the arithmetic when making this reduction.

Proposition 13. *Let $\varphi : R \to R'$ be a ring homomorphism. Then*

- *The* ***image*** *of φ, defined by $\operatorname{im}\varphi = \{\varphi(r) : r \in R\}$, is a subring of R'*
- *The* ***kernel*** *of φ, defined by $\ker\varphi = \{r \in R : \varphi(r) = 0\}$, is an ideal of R*

Theorem 14 (First Isomorphism Theorem)**.** *Let $\varphi : R \to R'$ be a ring homomorphism, and let π be the projection map $R \to R/\ker\varphi$ given by $a \mapsto a + \ker\varphi$. Then there exists an isomorphism*

$$\psi : R/\ker\varphi \to \operatorname{im}\varphi$$

such that $\psi \circ \pi = \varphi$. In particular, $R/\ker\varphi \cong \operatorname{im}\varphi$.

Polynomial Roots and Factorization

We next discuss some properties of polynomials over an arbitrary field.

Definition 15. Let R be a nonzero commutative ring. A nonzero element $x \in R$ is called a **zero-divisor** if there is another nonzero element $y \in R$ such that $xy = 0$. R is called an **integral domain** if it has no zero-divisors. An ideal of R is called **principal** if it is generated by a single element, and R is called a **principal ideal domain** if it is an integral domain and every ideal is principal.

Proposition 16. *For any field F, the polynomial ring $F[x]$ is a principal ideal domain.*

Lemma 17 (Polynomial Division Algorithm)**.** *Let F be a field, and let $f, g \in F[x]$ be polynomials. Then there exist unique polynomials $q, r \in F[x]$ with $\deg r < \deg g$ such that $f(x) = q(x)g(x) + r(x)$.*

Exercise 18. In $\mathbb{Q}[x]$, find the quotient and remainder polynomials q and r stipulated in the polynomial division algorithm for polynomials $f(x) = 2x^5 - 3x^4 - 3x^3 + x - 1$ and $g(x) = x^2 - 3x + 1$.

Lemma 19. *If F is a field, then a nonzero polynomial over F is invertible if and only if it is constant.*

Proof. Let $f \in F[x]$ be nonzero. If $f = \alpha$ for nonzero $\alpha \in F$, then it has inverse $g = \alpha^{-1}$. If f is non-constant, then it has positive degree, so its product with any nonzero polynomial must also have positive degree. This precludes the existence of an inverse. □

Lemma 20. *Let F be a field, let $f \in F[x]$ be a polynomial, and let $\alpha \in F$. Then $f(\alpha) = 0$ if and only if $(x - \alpha)$ divides f.*

Proof. If $(x-\alpha)$ divides f, then there is a polynomial g such that $f(x) = (x-\alpha)g(x)$, so we see that $f(\alpha) = (\alpha - \alpha)g(\alpha) = 0$. So suppose now that $f(\alpha) = 0$. Then by the polynomial division algorithm, there are polynomials $q, r \in F[x]$ such that $f(x) = q(x)(x - \alpha) + r(x)$, where $\deg(r) < \deg(x - \alpha) = 1$. Then $r(x)$ is a constant polynomial, $r(x) = \beta$ for $\beta \in F$. Then by assumption, we have

$$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = \beta$$

so $\beta = 0$, and we see that $f(x) = (x - \alpha)g(x)$, and thus $(x - \alpha)$ divides f. □

Proposition 21. *Let F be a field, and let $f \in F[x]$ be a nonzero polynomial of degree d. Then f has at most d roots in F.*

Proof. We proceed by induction on the degree of f. If f has degree 0, then it is a nonzero constant polynomial, and thus has zero roots.

Now suppose that f has positive degree d. If f has no roots, then we are done, so suppose that $\alpha \in F$ is a root of f. By the above lemma, we can write $f(x) = (x - \alpha)g(x)$ where g is a polynomial of degree $d - 1$, and by induction, g has at most $d - 1$ roots.

Since F is a field, it has no zero-divisors, so if $f(\beta) = 0$ for some $\beta \in F$, then either $\beta = \alpha$, or $g(\beta) = 0$. Thus the roots of f are α and the roots of g, giving at most d roots in total. □

Definition 22. Let F be a field, and let $f(x) = \sum_{n=0}^{d} a_n x^n$ be a polynomial in $F[x]$. The **formal derivative** of f is the polynomial

$$f'(x) = \sum_{n=0}^{d} n a_n x^{n-1}$$

Here, the integers n in the formula for the derivative are to be interpreted as the summation $1 + 1 + \cdots + 1$ of n copies of the multiplicative identity in F.

Exercise 23. Let α, β be elements of a field F, and let f, g be polynomials over F. Show that the formal derivative satisfies the following properties:

- *(Linearity)* $(\alpha f + \beta g)' = \alpha f' + \beta g'$
- *(Product Rule)* $(fg)' = f'g + fg'$
- *(Chain Rule)* $(f \circ g)' = (f' \circ g)g'$

Definition 24. Let F be a field, let $f \in F[x]$ be a polynomial, and let $\alpha \in F$. Then α is called a **multiple root** of f if $(x - \alpha)^2$ divides f.

Lemma 25. *Let F be a field, let $f \in F[x]$, and let $\alpha \in F$. Then α is a multiple root of f if and only if it is a root of both f and its derivative f'.*

Proof. If α is a multiple root, then we can write $f(x) = (x-\alpha)^2 g(x)$ for some polynomial g. Clearly α is a root of f, and we can compute using the chain rule that

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$$

which also has α as a root. For the other direction, suppose both f and f' have α as a root. Then we can write $f(x) = (x-\alpha)g(x)$ for some polynomial g, and we can compute

$$f'(x) = g(x) + (x-\alpha)g'(x)$$

Then we have $f'(\alpha) = g(\alpha) = 0$, so we can likewise write $g(x) = (x-\alpha)h(x)$ for some polynomial h, and so we obtain $f(x) = (x-\alpha)^2 h(x)$. □

Definition 26. Let F be a field, and let $f \in F[x]$ be a non-constant polynomial with coefficients in F. Then f is called **irreducible** (over F) if there is no way to write f as a product of two non-constant polynomials with coefficients in F.

Theorem 27 (Unique Factorization)**.** *Let F be a field, and let f be a nonzero polynomial over F. Then there exist monic irreducible polynomials $g_1, \ldots, g_k$ and a nonzero field element $u \in F$ such that*

$$f = u \prod_{i=1}^{k} g_i$$

and this representation is unique up to permutation of the indices.