Rings

Lukas Helminger

Mathematical Foundations of Cryptography – WT 2020/21

Outline

Rings

- Homomorphisms
- Characteristic
- Ideals
- Chinese Remainder Theorem

Polynomial rings

- Polynomials
- Long Division
- Irreducible Polynomials

Literature

The slides are based on the following books

- **Algebra of Cryptologists**, Alko R. Meijer
- **Algebra**, Gisbert Wüstholz
- **A Mind at Play: How Claude Shannon Invented the Information Age**, Jimmy Soni, Rob Goodman

Rings

Recap from Group Theory

A group is a set G together with a binary operation $* : G \times G \to G$, where $*$ is associative, has an identity element, and every element has an inverse element.

Examples:

- $\{\mathbb{Z}, +\}$
- $\{\mathbb{Z}_n, +\}$.

Rings

Definition (Ring)

A (commutative) ring is a set R together with two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$, such that the following is satisfied:

- $\{R, +\}$ is an abelian group.
- $\{R, \cdot\}$ is associative and has an identity element.
- $\forall r, s, t \in R : r(s + t) = rs + rt$ (distributive).

Note: We write 0 resp. 1 for the identity in $\{R, +\}$ resp. $\{R, \cdot\}$.

Rings: Examples

- $\{\mathbb{Z}, +, \cdot\}$
- $\{\mathbb{Z}_n, +, \cdot\}$

Why algebra matters

The current would pass through if only z were switched on, or if y and z were switched on, or if x and z were switched on, or if x and y were switched on, or if all three were switched on.

$$\begin{aligned} & x'y'z + x'yz + xy'z + xyz' + xyz \\ [\text{distributive}] \Rightarrow \quad & yz(x + x') + y'z(x + x') + xyz' \\ [x + x' = 1] \Rightarrow \quad & yz + y'z + xyz' \\ [\text{distributive}, y + y' = 1] \Rightarrow \quad & z + xyz' \\ [x + x'y = x + y] \Rightarrow \quad & z + xy \end{aligned}$$

Units

Definition (Unit)

Let R be a ring. An element $x \in R$ is called a unit of R if

$$\exists y \in R : xy = 1.$$

We denote the set of all units of R by R^*, which together with the multiplication is an abelian group.

- $\mathbb{Z}^* =?.$
- $\mathbb{Z}_n^* =?.$

Ring Homomorphisms

Recall: A map $\phi : G \to G'$ between two groups is called group homomorphism if

$$\phi(gh) = \phi(g)\phi(h) \quad \forall g, h \in G.$$

Definition (Ring homomorphism)

A map $\phi : R \to S$ between to rings is called (ring) homomorphism if for all $r, s \in R$:

- $\phi(r + s) = \phi(r) + \phi(s)$,
- $\phi(rs) = \phi(r)\phi(s)$,
- $\phi(1_R) = 1_S$.

Note: If ϕ is an injective homomorphism, we sometimes call it embedding.

Ring Homomorphisms: Examples

- The "modulo n map"

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ a &\longmapsto a + n\mathbb{Z} \end{aligned}$$

  is a ring homomorphism.

- Let R and S be rings such that $R \subset S$. Then we always have the trivial embedding:

$$\begin{aligned} \phi : R &\longrightarrow S \\ r &\longmapsto r \end{aligned}$$

Characteristic: Examples

The characteristic of a ring R is the smallest $n \in \mathbb{N}$ such that $n \cdot 1 = 1 + \cdots + 1 = 0$.

- $\text{char}(\mathbb{Z}) = 0$.
- $\text{char}(\mathbb{Z}_n) = n$, because $\bar{0} = n \cdot \bar{1}$.
- There exists infinite rings with a non-zero characteristic (see section about polynomial rings).

Frobenius Homomorphism

Proposition (The Freshman's Dream)

Let p be prime and let R be a ring of characteristic p. Further, let $x, y \in R$, then

$$(x+y)^p = x^p + y^p.$$

Thereby, the map

$$\begin{aligned} \mathrm{Frob}_p : R &\longrightarrow R \\ x &\longmapsto x^p \end{aligned}$$

is a ring homomorphism, called the Frobenius homomorphism.

Note: Frob_p can be used as indicator for weaknesses of elliptic curves.

Ideals

A subset $R' \subset R$ of a ring R is called a subring of R if

- $\{R', +\}$ is a subgroup of $\{R, +\}$,
- R' is closed under multiplication.

Definition (Ideal)

Let R be a ring. A subring $I \subset R$ is called an ideal in R if

$$\forall r \in R \forall a \in I : ar \in I.$$

Ideal: Examples

- $n\mathbb{Z}$ in $\mathbb{Z}$.
- $\mathbb{Z}$ is only a subring in $\mathbb{R}$. Why?

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Let $a_1, \ldots, a_k \in \mathbb{Z}$ and $n_1, \ldots, n_k$ pairwise coprime. Then there exists an element $x \in \mathbb{Z}$ such that

$$\begin{aligned} x &\equiv a_1 \mod (n_1) \\ &\vdots \\ x &\equiv a_k \mod (n_k). \end{aligned}$$

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

Decomposition

Corollary

Let $m_1, \ldots, m_n \in \mathbb{N}$ pairwise co-prime with $m = m_1 m_2 \cdots m_n$. It follows that

$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}.$$

- $m_1 = 4, m_2 = 5, m_3 = 3$
- $m_1 = 7, m_2 = 2, m_3 = 3$
- $m_1 = 2, m_2 = 5, m_3 = 6$

Quotient Rings

Recall: Let $H \subset G$ be a subgroup of G. Then $G/H = \{gH : g \in G\}$ with the operation $(gH, g'H) \mapsto (gg'H)$ is the corresponding quotient group.

Definition (Quotient Ring)

Let R be a ring and let $I \subset R$ be an ideal of R. The quotient group $R/I = \{r + I : r \in R\}$ together with the following multiplication

$$\begin{aligned} \cdot : R/I \times R/I &\longrightarrow R/I \\ (r + I, r' + I) &\longmapsto (rr') + I. \end{aligned}$$

is called a quotient ring.

$R = \mathbb{Z}, I := (5)\mathbb{Z} \subset \mathbb{Z}$

$$R/I = \mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5 = \{a + 5\mathbb{Z} \in \mathbb{Z}/5\mathbb{Z} \mid a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}.$$

Chinese Remainder Theorem for Ideals

Notation: In analogy to the integers we write $r \equiv s \mod I$, if $r - s \in I$.

Theorem (Chinese Remainder Theorem for Ideals)

Let R be a ring, and let $x_1, \ldots, x_n \in R$. Further, let $I_1, \ldots, I_n \subset R$ be ideals of R with $I_i + I_j = R$, for $i \neq j$. Then there exists an element $x \in R$ such that

$$x \equiv x_i \mod I_i, \quad \text{for } 1 \leq i \leq n.$$

What you should remember!

- Definition of ring.
- Definition of an ideal.
- Chinese Remainder Theorem.

Polynomial rings

Polynomials

Definition (Polynomial)

Let R be a ring. We define a polynomial over R as a finite formal sum of the form

$$f(X) = \sum_{i=0}^{n} a_i X^i,$$

where $a_i \in R$, called the coefficients of f. Further, we assume that $a_n \neq 0 \in R$, except all a_i's are zero.

- The leading coefficient of $f(X)$ is a_n.
- The constant term of $f(X)$ is a_0.
- The degree of $f(X)$ is $\deg f(X) = n$.

The symbol X is called indeterminate or variable.

Polynomials: Examples

Let $R = \mathbb{Z}$, then

$$f(X) = -3X^{10} + 20X^7 + 4X^3 + 8$$

is a polynomial over $\mathbb{Z}$, with

- leading coefficient -3,
- constant term 8, and
- $\deg f(X) = 10$.

Note:

$$g(X) = \frac{1}{2}X^2 - X + 1$$

is a polynomial over $\mathbb{Q}$, but not over the smaller ring $\mathbb{Z}$.

Binary Operations on Polynomials

Let R be a ring and let $f(X) = \sum_{i=0}^{n} a_i X^i$ and $g(X) = \sum_{i=0}^{m} b_i X^i$ be two polynomials over R. (Assume w.l.o.g $n > m$, and set $b_i = 0$ for $m < i \leq n$)

We define the polynomial addition componentwise:

$$f(X) + g(X) := \sum_{i=0}^{n} (a_i + b_i) X^i.$$

Multiplication is defined as follows

$$f(X)g(X) := \sum_{j=0}^{m+n} c_j X^j, \quad \text{with } c_j := \sum_{i=0}^{j} a_i b_{j-i}.$$

Binary Operations on Polynomials: Examples

- Consider polynomials over $\mathbb{Z}$, i.e. all polynomials with integer coefficients. Let $f(X) = 1 + X^2, g(X) = 1 + X^2 + X^4 \in \mathbb{Z}[X]$. Then

$$f(X) + g(X) = 2 + 2X^2 + X^4$$
$$f(X)g(X) = 1 + X^2 + X^4 + X^2 + X^4 + X^6 = 1 + 2X^2 + 2X^4 + X^6$$

- Consider polynomials over $\mathbb{Z}_2$, i.e. all polynomials with coefficients in $\{\bar{0}, \bar{1}\}$. Let $f(X) = \bar{1} + X^2, g(X) = \bar{1} + X^2 + X^4 \in \mathbb{Z}_2[X]$. Then

$$f(X) + g(X) = \bar{2} + \bar{2}X^2 + X^4 = X^4$$
$$f(X)g(X) = \bar{1} + X^2 + X^4 + X^2 + X^4 + X^6 = \bar{1} + X^6$$

Polynomial Rings

Definition (Polynomial ring)

Let R be a ring. The polynomial ring $R[X]$ over R is defined as the set of all polynomials over R, together with the operations defined above.

Let R be a ring.

- The proof that the polynomial ring $R[X]$ actually is a ring, is not difficult but tedious and messy.
- The construction of the polynomial in one variable can be generalized to the polynomial ring in n variable $R[X_1, \ldots, X_n]$.
- For elliptic curves the polynomial rings $R[X, Y]$ and $R[X, Y, Z]$ are important.

Polynomial vs. Polynomial function

Given $f(X)$ with coefficients in R, we can view $f(X)$ as either

- a polynomial, if we consider X merely as a placeholder,
- or as a polynomial function, if we allow X to take values in R (or a overring of R).

Example: Let $f(X) = 2X^2 - 3 \in \mathbb{Z}[X]$ and $s = \frac{1}{2} \in \mathbb{Q}$. Then we can evaluate $f(X)$ at s and get $-\frac{5}{2} \in \mathbb{Q}$.

Long Division

The greatest common divisor of a and b (write $\gcd(a,b)$) is a divisor d of a and b, which gets divided by every common divisor of a and b.

There exists a greatest common divisor $d(X) = \gcd(f(X), g(X))$. It is computed in analogy to the integers.

Long Division: Let $f(X) = X^5 + X^4 + X^2 + 1, g(X) = X^4 + X^2 + X + 1 \in \mathbb{Z}_2[X]$:

$$\begin{aligned} X^5 + X^4 + X^2 + 1 &= (X+1)(X^4 + X^2 + X + 1) + (X^3 + X^2) \\ X^4 + X^2 + X + 1 &= (X+1)(X^3 + X^2) + (X+1) \\ X^3 + X^2 &= X^2(X+1) + 0 \end{aligned}$$

This shows that

$$\gcd(f(X), g(X)) = X + 1 \in \mathbb{Z}_2[X].$$

Irreducible Polynomials

Definition (Irreducible Polynomial)

A non-constant polynomial $f(X) \in R[X]$ is called irreducible in $R[X]$ if it cannot be factored in two non-constant polynomials with coefficients in R.

- $X^5 + X^4 + 1 \in \mathbb{Z}_2[X]$ is reducible, since $X^5 + X^4 + 1 = (X^2 + X + 1)(X^3 + X + 1)$.
- $f(X) = X^2 + X + 1 \in \mathbb{Z}_2[X]$ is irreducible. Assume to the contrary $f(X)$ is reducible, i.e. $f(X) = (X - \alpha)(X - \beta)$, with $\alpha, \beta \in \mathbb{Z}_2$. But then $f(\alpha) = 0$, a contradiction.
- Irreducibility highly depends on the underlying field, e.g. $X^2 + 1$ is irreducible in $\mathbb{R}[X]$, but reducible in $\mathbb{C}[X]$, since $X^2 + 1 = (X - i)(X + i)$.