Rings

Lukas Helminger

Mathematical Foundations of Cryptography – WT 2019/20

Outline

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 monoid is a set M together with a binary operation $* : M \times M \to M$, where $*$ is associative and has an identity element.

If every element of a monoid $\{G, *\}$ has an inverse element, we call it a group.

Examples:

- $\{\mathbb{Z}, +\}$ and $\{\mathbb{Z}_n, +\}$ are abelian groups.
- $\{\mathbb{Z}, \cdot\}$ and $\{\mathbb{Z}_n, \cdot\}$ are monoids.

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 a (commutative) monoid.
- $\forall r, s, t \in R : r(s + t) = rs + rt$ (distributive).

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

Rings: Examples

- The integers $\{\mathbb{Z}, +, \cdot\}$ form a commutative ring.
- The set of residue classes modulo a given integer $\{\mathbb{Z}_n, +, \cdot\}$ form a ring.
- Let M be any set and let R be a ring, then set of all maps from M to R, denoted by $R^M := \{f : M \to R\}$ is a ring with the following operations:

$$
\begin{aligned}
+ : R^M \times R^M &\longrightarrow R^M \\
(f, g) &\longmapsto (f + g) : M \to R \\
&\qquad\qquad x \mapsto (f + g)(x) := f(x) + g(x)
\end{aligned}
$$

In analogy to the addition, we define the multiplication.

Why algebra matters

Say that a certain function in the circuits would allow the current to pass through—would output a 1, in Shannon's terms—depending on the state of three different switches, x, y, and z.

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.

- The units of the integers are $\mathbb{Z}^* = \{-1, 1\}$.
- We already saw that $\mathbb{Z}_n^* = \{a + n\mathbb{Z} \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$.

If $R^* = R \setminus \{0\}$, i.e. every element of the ring R except 0 has an multiplicative inverse, then we call R a field.

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:

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

Subrings

Recall: A subgroup of $\{G, *\}$ is a non-empty subset, which is closed under $*$ and taking inverses.

Definition (Subring)

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.

We denote by $\mathbb{P}$, the subring generated by the multiplicative identity element 1, i.e.

$$\mathbb{P} = \{n \cdot 1 \mid n \in \mathbb{N}\}.$$

Characteristic

Theorem

For every non-trivial ring R, the subring $\mathbb{P}$ is either isomorphic to $\mathbb{Z}$ or to $\mathbb{Z}_n$.

Definition (Characteristic)

The characteristic of a ring R is defined as

$$\operatorname{char}(R) := \begin{cases} 0 & \text{if } \mathbb{P} \cong \mathbb{Z}, \\ n & \text{if } \mathbb{P} \cong \mathbb{Z}_n. \end{cases}$$

We can also think of the $\operatorname{char}(R)$ as the smallest $n \in \mathbb{N}$ such that $n \cdot 1 = 1 + \cdots + 1 = 0$.

Characteristic: Examples

- $\text{char}(\mathbb{Z}) = 0$.
- $\text{char}(\mathbb{Z}_n) = n$, 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

Definition (Ideal)

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

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

Examples:

- Consider $n\mathbb{Z} \subset \mathbb{Z}$ for a fixed integer n. We already saw that $\{n\mathbb{Z}, +\}$ is a subgroup of $\mathbb{Z}$. To be an ideal it is left to check that $n\mathbb{Z}$ is closed under multiplication with integers. Let $r \in \mathbb{Z}$ and $kn \in n\mathbb{Z}$, then

$$r \cdot kn = (rk) \cdot n \in n\mathbb{Z}.$$

- The integers $\mathbb{Z}$ are obviously a subring of the reals $\mathbb{R}$. Since $\sqrt{2} \in \mathbb{R}$ but $\sqrt{2} \cdot 3 \notin \mathbb{Z}$, the integers do not form an ideal in $\mathbb{R}$.

Principal Ideals

We just saw that the ideal $n\mathbb{Z} \subset \mathbb{Z}$ is generated by the single integer n. This construction can be generalized to arbitrary rings.

Definition (Principal Ideal)

Let R be a ring. A principal ideal generated by $a \in R$ consists of all the multiples of a

$$(a) := aR = \{ar : r \in R\}.$$

If every ideal in R is a principal ideal, we call R a principal ideal domain (PID).

Proposition

The integers $\mathbb{Z}$ are a principal ideal domain.

Greatest Common Divisor

Let $a, b \in R$. We say that a divides b (and write $a \mid b$) if

$$\exists r \in R : b = ra.$$

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.

Proposition

Let R be a PID and let $a, b \in R$. Then there always exists $\gcd(a, b)$.

Sum, Intersection & Multiplication of Ideals

Let R be a ring and let $I, J \subset R$ be two ideals of R. Then the following sets are again ideals of R

- The intersection $I \cap J$

  Example: $R = \mathbb{Z}$ and $I = m\mathbb{Z}, J = n\mathbb{Z}$ for $m, n \in \mathbb{Z}$, then
  $$I \cap J = m\mathbb{Z} \cap n\mathbb{Z} = \operatorname{lcm}(m, n)\mathbb{Z}.$$

- The sum $I + J := \{a + b \mid a \in I, b \in J\}$.

  Example: $R = \mathbb{Z}$ and $I = m\mathbb{Z}, J = n\mathbb{Z}$ for $m, n \in \mathbb{Z}$, then
  $$I + J = m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}.$$

- The sum $I \cdot J := \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbb{N}\}$.

  Example: $R = \mathbb{Z}$ and $I = m\mathbb{Z}, J = n\mathbb{Z}$ for $m, n \in \mathbb{Z}$, then
  $$I \cdot J = m\mathbb{Z} \cdot n\mathbb{Z} = mn\mathbb{Z}.$$

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.

Consider $R = \mathbb{Z}$ and the ideal $I := (n) \subset \mathbb{Z}$, for some $n \in \mathbb{Z}$. Then the corresponding quotient ring is the ring of all residue classes modulo n

$$R/I = \mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z} \mid a \in \mathbb{Z}\}.$$

Chinese Remainder Theorem

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

Theorem (Chinese Remainder Theorem)

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

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

Theorem (Chinese Remainder Theorem for the Integers)

Let $x_1, \dots, x_n \in \mathbb{Z}$. Further, let $m_1\mathbb{Z}, \dots, m_n\mathbb{Z} \subset R$ be ideals of $\mathbb{Z}$ with $m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$ (i.e. $\gcd(m_i, m_j) = 1$), for $i \neq j$. Then there exists an element $x \in \mathbb{Z}$ such that

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

Decomposition

Corollary

Let $I_1, \dots, I_n \subset R$ be ideals of R with $I_i + I_j = R$, for $i \neq j$. Then there is a canonical isomorphism

$$R/\left(I_1 \cap \cdots \cap I_n\right) \cong R/I_1 \times \cdots \times R/I_n.$$

Example: $R = \mathbb{Z}$ and $m_1, \dots, m_n \in \mathbb{N}$ pairwise co-prime with $m = m_1 m_2 \cdots m_n$. It follows that

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

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 from importance.

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).

More formally, let $R[X]$ be a polynomial ring over the ring R and let $S \supset R$ be a ring. For every $s \in S$, we introduce the map

$$\phi_s : R[X] \longrightarrow S, \quad \sum_{i=0}^{n} a_i X_i \longmapsto \sum_{i=0}^{n} a_i s^i,$$

which is called evaluation homomorphism.

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 $-\frac{5}{2} \in \mathbb{Q}$.

Polynomial rings over fields

Theorem

Let K be field. Then $K[X]$ is a PID, i.e.

$$\forall I \subset K[X] \text{ ideal } \exists f(X) : I = \{g(X)f(X) \mid g(X) \in K[X]\}.$$

Note: $f(X)$ in the last theorem is not unique. Therefore one often chooses the unique monic polynomial (leading coefficient equals 1).

Example: The set of all polynomials that vanish in a given set $S \subset \mathbb{C}$, i.e.,

$$I_S := \{f \in \mathbb{C}[X] : f(s) = 0 \quad \forall s \in S\}$$

is an ideal. Since $\mathbb{C}[X]$ is a PID, we know that I is generated by a single polynomial.

Long Division

Let $K[X]$ be a polynomial ring over a field K and let $f(X), g(X) \in K[X]$ be two polynomials. The last theorem implies that there exists a greatest common divisor $d(X) = \gcd(f(X), g(X))$. It is computed in analogy to the integers.

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

$$X^5 + X^4 + X^2 + 1 = (X+1)(X^4 + X^2 + X + 1) + (X^3 + X^2)$$
$$X^4 + X^2 + X + 1 = (X+1)(X^3 + X^2) + (X+1)$$
$$X^3 + X^2 = X^2(X+1) + 0$$

This shows that

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

Irreducible Polynomials

Definition (Irreducible Polynomial)

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

- $X^5 + X^4 + 1 \in \mathbb{Z}_2[X]$ 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 $X^2 + 1 = (X - i)(X + i)$.

CRT for Polynomials

Theorem (CRT for Polynomials)

Let K be a field and let $a_1(X), \ldots, a_n(X) \in K[X]$. Further, let $e_i(X) \in K[X]$ be distinct irreducible polynomials, for $i = 1, \ldots, n$. Then there exists a polynomial $f(X) \in K[X]$ such that

$$f(X) \equiv a_i(X) \mod e_i(X),$$

for $1 \leq i \leq n$.