TD ACCQ 201

Julien Béguinot, Duong Hieu Phan

Télécom Paris

1 Reminder

Definition 1. A **ring** $(A, +, \times)$ is a set A equiped with two operations $+$ and $\times$ such that
- $(A, +)$ is an Abelian group
- there exists a neutral element 1_A in A for $\times$
- $\times$ is associative
- $\times$ is distributive on $+$

If $\times$ is commutative the ring is said to be a **commutative ring**.

Definition 2. A left (resp right) **ideal** $\mathcal{I}$ of the ring A is an additive subgroup of A stable by by multiplication by an element of A on the left (resp right). If $\mathcal{I}$ is both a right and a left ideal it is an ideal.

An ideal $\mathcal{I}$ is said to be **principal** if there exists an element $x \in A$ such that $\mathcal{I} = AxA$. We use the notation (x) to designate the corresponding ideal.

More generally $(x_1, \dots, x_n)$ is the smallest ideal containing (x_i) for $i = 1, \dots, n$. An ideal that can be expressed this way is said to be of **finite type**.

Definition 3. A **field** is a commutative ring with no non-trivial ideal. In other words every non-zero elements of the ring is invertible.

Definition 4. An **integral ring** is a commutative ring verifying the zero product rule i.e.

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

Definition 5. An integral ring is said to be **principal** if all its ideals are principal.

Theorem 1. $(\mathbb{Z}, +, \times)$ *is a principal ring.*

Definition 6. Let A be an integral ring and $a, b \in A$.
- a is said to be **irreducible** if it is non zero, non invertible and for all decomposition $a = uv$ then either v or u is invertible.
- a and b are said to be **associated** if there exists an invertible element u such that $a = ub$.
- $p \in A$ is said to be **prime** if it is non zero, non invertible and for all product ab if $p|ab$ then $p|a$ or $p|b$.

The integral ring A is said to be a **factorial** ring if every elements of A which is non-zero and non invertible is a product of prime elements of A.

Definition 7. The ideal I of the commutative ring A is said to be prime if

$$\forall (a, b) \in A^2, ab \in I \implies (a \in I \text{ or } b \in I).$$

This is equivalent to say that the quotient ring A/I is integral.

Definition 8. An **Euclidean** ring A is an integral ring that can be endowed with a function[1] $f : A\backslash\{0\} \mapsto \mathbb{N}$ such that

- $f(a) = 0$ if and only if $a = 0$
- $\forall a \in A, \forall b \in A\backslash\{0\}, \exists q, r \in A^2, f(r) < f(b), a = bq + r$

Definition 9. The commutative ring A is said to be **Noetherian** if every ideal of A is of finite type. This is equivalent to say that every sequence of ideal of A increasing for the inclusion is stationary.

Definition 10. An ideal I of the ring A is **maximal** if and only if A/I is a field. Equivalently it is contained in exactly two ideals: itself and the whole ring.

Definition 11. Let A be a ring. Let $f : n \in \mathbb{Z} \mapsto n \cdot 1_A \in A$. The f is a ring morphism from the principal ring $\mathbb{Z}$ to A. The **charachteristic** of A is defined as:

- if $\mathrm{Ker}(f) = \{0\}$ then it is zero;
- else there exists a unique natural integer c such that $\mathrm{Ker}(f) = c\mathbb{Z}$ and it is c.

Proposition 1. *If A is a ring and I an ideal of A then A/I is integral if and only if I is prime i.e. $\forall a, b \in A, ab \in I \implies (a \in I \text{ or } b \in I)$.*

Theorem 2. *A finite field is commutative.*

Theorem 3. *Let $G \subset K^*$ be a finite subgroup of the group of invertible of the field K. Then G is a cyclic group. As a consequence $\mathbb{Z}_p^*$ is cyclic.*

Theorem 4 (Euler)**.** *Let φ be Euler indicator function and $n > 1$. If k is coprime with n then $k^{\varphi(n)} = 1 \,(\mathrm{mod}\, n)$.*

Definition 12 (Legendre Symbol)**.** Let p be a prime odd number. The Legendre symbol (n/p) is defined as

$$\left(\frac{n}{p}\right) : \begin{cases} 0 \text{ if } p \text{ divides } n \\ +1 \text{ if } p \text{ does not divide } n \text{ and } n \text{ is a square mod } p \\ -1 \text{if } p \text{ is not a square mod } p \end{cases} .$$

Theorem 5 (Quadratic Residuosity)**.** *Let $a \in \mathbb{Z}, p \not| a$, p odd prime.*

$$a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \,(\mathrm{mod}\, p).$$

Definition 13 (Jacobi Symbol)**.** Let $a \in \mathbb{Z}$ and $n \in 2\mathbb{N} + 1$. We assume that $n = \prod_{i=1}^{k} p_i$. Then the Jacobi symbol generalizes the Legendre symbol as

$$\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i}\right).$$

It verifies the following properties:

- it is zero if and only if a and n are not co-prime
- it is multiplicative in a and in n
- if $a = b \,(\mathrm{mod} n)$ then $(a/n) = (b/n)$.
-

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \qquad \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \qquad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

Theorem 6 (Krull)**.** *Let $\mathcal{I}$ be a non trivial ideal of the commutative ring A. There exists at least one maximal ideal of A that contains $\mathcal{I}$. This property is a consequence of the axiom of choice.*

[1] Termed stathme in French

2 Exercices

Exercice 1. *Let A be a commutative ring.*
- *If A contains only the two trivial ideal then it is a field.*
- *If A is integral and contains a finite number of ideals then it is a field.*

Exercice 2. *Let A be a principal ring.*

- *Show that if every sequence of ideal of A deacreasing for the inclusion is stationary then A is a field.*
- *Show that every increasing sequence of ideal of A is stationnary.*

Exercice 3. *Is the ring of function from $\mathbb{R}$ to $\mathbb{R}$ an integral ring ? Is the ring of continuous function from $\mathbb{R}$ to $\mathbb{R}$ a Noetherian ring ?*

Exercice 4. *Let $n \geqslant 2$, show that every ideal of $\mathbb{Z}_n$ is principal. Is $\mathbb{Z}_n$ principal ?*

Exercice 5. *Let A be a ring and P a polynomial in $A[X]$. $a \in A$ is said to be a zero/root of P if $P(a) = 0$. Show that a is a zero of P if and only if $X - a | P$. Show that if A is integral then any non zero polynomial P of degree n admits at most n zero in A.*

Exercice 6. *Let A be an integral ring. If $p \in A$ is prime then it is irreducible.*

Exercice 7 (Characteristic of a Ring)**.** *Let A be a ring of finite chararchteristic N. Show that:*
- $\forall a \in A, N \cdot a = 0$.
- *If A is integral then N is prime.*
- *If A is integral then $X \mapsto x^N$ is ring morphism.*

Exercice 8. *Let A be a principal ring. p irreducible $\implies$ p prime and p irreducible $\implies$ (p) maximal $\implies$ $A/(p)$ field $\implies$ p prime.*

Exercice 9. *Let A be a ring and $\mathcal{Z}(A)$ be the set of elements of A that commutes with all elements of A. Show that $\mathcal{Z}(A)$ called the center of A is a subring of A.*

Exercice 10. *We investigate some properties of the famoius Gauss integer ring.*
- *Show that $\mathbb{Z}[i]$ is a ring*
- *Let $N : z \in \mathbb{C} \mapsto z\bar{z} \in \mathbb{R}^+$.*
  - *Show that N is multiplicative.*
  - *Show that if $z \in \mathbb{Z}[i]$ then $N(z) \in \mathbb{N}$.*
  - *Let $z \in \mathbb{Z}[i]$ be invertible. Show that $N(z) = 1$.*
  - *List the invertible elements of $\mathbb{Z}[i]$.*
- *Show that if $z \in \mathbb{C}$ then there exists $w \in Z[i]$ such that $|z - w| < 1$.*
- *Let $u, v \in \mathbb{Z}[i]$ show that there exists $q, r \in Z[i]$ such that $u = qv + r$ with $|r| < |v|$. Is $\mathbb{Z}[i]$ euclidean ?*
- *Show that $\mathbb{Z}[i]$ is principal.*