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 $(x_1, \ldots, x_n)$ is the smallest ideal containing (x_i) for $i = 1, \ldots, n$. 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 $k^{\varphi(n)} = 1 \pmod n$.*

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.*

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

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 $a = b \pmod n$ 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.*

Solution 1.

- Let $x \in A, x \neq 0$, we have to prove that x is invertible. Since $x \neq 0$, (x) cannot be the empty ideal hence it must be the full ring. In particular there must exists $a \in A$ such that $xa = 1$ i.e. x is invertible.
- Let $x \in A, x \neq 0$, we have to prove that x is invertible. Let $I_n = (x^n)$ since the is a finite number of ideal there must exists $n < p$ such that $I_p = I_n$. In particular we have $a \in A$ such that $x^n = x^p a$. But then $x^n(1 - x^{p-n}a) = 0$ and since A is integral $x^{p-n}a = 1$ i.e. x is invertible of inverse $x^{p-n-1}a$.

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.*

Solution 2.

- Let $x \in A, x \neq 0$, we have to prove that x is invertible. Let $I_n = (x^n)$ then clearly the sequence of ideal is deacreasing for the inclusion. Hence we have a rank p such that $I_p = I_{p+1}$ in particular we have $a \in A$ such that $ax^{p+1} = x^p$ i.e. $x^p(1 - ax) = 0$. This implies $ax = 1$ i.e. x is invertible.
- Let (I_i) be a sequence of increasing ideals. Then $I = \cup I_i$ is an ideal. Since A is principal so is I and there exists $a \in A$ such that $I = (a)$. Necessarly there must exist a rank N such that $a \in I_N$. But then $(a) \subset I_N \subset I_{N+1} \subset \ldots \subset I = (a)$ which concludes the proof.

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 ?*

Solution 3. No, let A be a non empty intervall and consider $f = 1_A$ and $g = 1_{A^c}$ then $fg = 0_{\mathbb{R} \mapsto \mathbb{R}}$ while f, g are non zero. No, again consider the increasing sequence of ideal $I_n = \{f | x \geqslant n \implies f(x) = 0\}$ which is non stationary.

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

Solution 4. Let $\mathcal{I}$ be an ideal of $\mathbb{Z}_n$. Let $\mathcal{J} = \{n \in \mathbb{Z} | \bar{m} \in \mathcal{I}\}$. Clearly $\mathcal{J}$ is an ideal of $\mathbb{Z}$ which is principal so $\mathcal{J} = a\mathbb{Z}$ for some $a \in \mathbb{Z}$ and we can check that $\mathcal{I} = \bar{a}\mathbb{Z}_n$. $\mathbb{Z}_n$ is not necessarly principal. This happens if $\mathbb{Z}_n$ is integral which happens if n is prime.

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.*

Solution 5. If $X - a | P$ then $P = (X - a)Q$ so $P(a) = (a - a)Q(a) = 0Q(a) = 0$ and a is a zero of P. Conversly assume that a is a zero of P. We write the division of P by $X - a$ so that $P = Q(X - a) + c$ where $c \in A$. But $0 = P(a) = (a - a)Q(a) + c = c$ so $c = 0$ i.e. $P = (X - a)Q$ i.e. $X - a | P$. For the second point we can proceed by induction. Let P a polynomial with n disctincts roots $a_1, \ldots, a_n$. a_n is a zero of P so $X - a_n | P$ i.e. $P = (X - a_n)Q$. But $a_1, \ldots, a_{n-1}$ are zero of P and $a_n - a_i \neq 0$ so $a_1, \ldots, a_{n-1}$ are zero of Q. By induction, we obtain that $(X - a_1) \ldots (X - a_n) | P$. In particular the degree of P is at least n. This in turns imply that a polynomial of degree n admits at most n roots.

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

Solution 6. Let p be a prime element of A. Let u, v be two elements in A such that $p = uv$. In particular $p|p = uv$ so $p|uv$. By primality of p we obtain that $p|u$ or $p|v$. Since A is commutative we can assume without loss of generality that $p|u$ i.e. $u = kp$. Then $p = uv = kpv = kvp$. In particular $p(1 - kv) = 0$ so $1 = kv$ since A is integral. This show that v is invertible. Hence p 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.*

Solution 7. Since $N1_A = 0$ we have $Na = 0a = 0$. Let us assume that A is integral and $N = pq$ we show that either p or q is equal to 1. We have $0 = N1_A = pq1_A = (p1_A)(q1_A)$. But A is integral so this implies that either $p1_A$ or $q1_A$ is zero. By the minimality of the characteristic this implies that $p = N$ and $q = 1$ or $p = 1$ and $q = N$. To show that $x \mapsto x^N$ is a ring morphism we have to show that the mapping is additive (the other properties of the morphism are easily verified). Let $a, b \in A$. Since A is integral it is by definition commutative and Newtown formula holds

$$(a + b)^N = b^N + \sum_{k=1}^{N-1} \binom{N}{k} a^k b^{N-k} + a^N.$$

The results follows since $p|\binom{N}{k}$ for $k \neq 0, k \neq N$. Indeed,

$$p! = \binom{N}{k} k!(N - k)!.$$

and p divides $p! = \binom{N}{k} k!(N - k)!$. SInce p cannot divide $k!(N - k)!$ and it is prime it necessary divides $\binom{N}{k}$.

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

Solution 8.

- We assume that p is ireducible and show that (p) is maximal. Let $\mathcal{I}$ be an ideal of A containing (p). Since A is principal $I = (x)$ for some $x \in A$. As consequence there exists $y \in A$ such that $p = xy$. Since p is irreducible it follows that either x or y in invertible. If x is invertible then $I = A$ else y is invertible and $x \sim p$ i.e. $I = (p)$. This proves that (p) is maximal.
- By definition an ideal I is maximal if A/I is a field.
- A/I is integral if and only if I is prime. So if (p) was not prime then $A/(p)$ would not be integral which is absurd.

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.*

Solution 9. $1_A \in \mathcal{Z}(A)$. If a, b commutes with every elements of A then so does $a - b$. Further if a, b commutes with every elements of A then ab also does.

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.*

Solution 10. It is a ring seen a a subring of $\mathbb{C}$. Since $N(z) = |z|^2$ it is multiplicative. If $z = a + bi \in Z[i]$ then $N = (z = a + bi) = a^2 + b^2$ is an integer. If $z \in Z[i]$ is invertible then $N(z)N(z^{-1})N(zz^{-1}) = N(1) = 1$. Hence $N(z)|1$ and is positive i.e. $N(z) = 1$. From that we can deduxe that the invertible elements of $Z[i]$ are $1, -1, i, -i$. The approximation can be achieved by replacing the real and imaginary part by the closet integer. We can find q as shown before such that $|\frac{u}{v} - q| < 1$ and let $r = v(\frac{u}{v} - q)$. The decomposition is not unique hence this division is not euclidean. We show that $\mathbb{Z}[i]$ is principal. Let I be a non trivial ideal of $\mathbb{Z}[i]$. Let a be the a smallest non-zero element of I in the sense of $|\cdots|$ which is well defined since $\mathbb{Z}[i]$ is discrete. Necessarily $I = (a)$. The inclusion $(a) \subset I$ is clear. It remains to show the other direction. Let $z \in I$. By the division by a introduced before we have $z = qa + r$ with $|r| < |a|$. But $r = z - qa \in I$ so necessarily $r = 0$ (else it contradicts the minimality of a). This implies that $z \in (a)$. In conclusion $\mathbb{Z}[i]$ is principal.

Exercice 11. *Compute* $\left(\frac{2585}{5031}\right), \left(\frac{122}{237}\right)$.

Solution 11. Use the relation on Jacobi coefficient to reduce the numerator and denomiator by successive euclidean division.

Exercice 12. *Determine when $q = 3, 11$ is a square modulo p.*

Solution 12. We use the quadratic residue criterium from Euler. For example for $q = 3$. We know that q is a square modulo p if and only if $(3/p) = 1$. But $(3/p) = (p/3)(-1)^{\frac{p-1}{2}}$. If $p - 1 = 4k$ then we need $(p/3) = 1$ i.e. $p = 3k' + 1$. It follows by Euclide lemma that in this case we need $p = 12k'' + 1$. If $p - 3 = 4k$ then we need $(p/3) = -1$ i.e. $p = 3k' + 2$. By the chinese reminder theorem we copnclude that necessarily $p = 3(3^{-1}(4))3 + 4(4^{-1}(3))2 + 12k'' = 9 + 4 + 12k'' = 1 + 12k'''$. In any case we obtain that 3 is a square modulo p if and only if p is equal to 1 modulo 12. Apply the same method to $q = 11$.