Fall 2024

# Summary: Rings

## 1 Definition and first examples

**Definition 1.1.** A *ring* is a set $A$ with two internal binary operations (addition and multiplication) satisfying the axioms:

1. $A$ is an abelian group with respect to addition. We will denote the corresponding neutral element by 0.
2. The multiplication is associative: $(ab)c = a(bc)\ \forall a, b, c \in A$ and there is an neutral element for multiplication, that will be denoted by 1: $1a = a1 = a\ \forall a \in A$.
3. Distributivity holds: $(a + b)c = ac + bc$ and $a(b + c) = ab + ac\ \forall a, b, c \in A$.

**Definition 1.2.** The ring $A$ is called *commutative* if $ab = ba\ \forall a, b \in A$.

## 2 Zero divisors. Integral domains

What is the most notable difference between (real, integer, rational, complex) numbers and commutative rings? If $x, y \in \mathbb{R}$ and $x \neq 0, y \neq 0$, then $xy \neq 0$. This is not necessarily true for rings.

**Definition 2.1.** Let $A$ be a ring. An element $a \in A$ is called a *left zero divisor* if there exists $x \in A$, $x \neq 0$, such that $ax = 0$. Similarly, an element $b \in A$ is called a *right zero divisor* if there exists $y \in A$, $y \neq 0$, such that $yb = 0$. An element that is both a left and a right zero divisor is called a *two-sided zero divisor.*

**Remark 2.2.** (a) The element 0 is a left and right zero divisor in any ring.

(b) In a commutative ring, any zero divisor is two-sided.

**Definition 2.3.** A zero divisor that is different from 0 is called a *nontrivial* zero divisor.

**Definition 2.4.** Let $A$ be a ring. If $A$ has no nontrivial zero divisors, it is called a *domain*.

**Definition 2.5.** A commutative ring whose only zero divisor is 0 is called an *integral domain*.

**Proposition 2.6.** *The ring $A = \mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if $n = p$ is a prime.*

**Proposition 2.7.** *Let $A$ be a ring. Then $A$ is a domain if and only if the equation $ab = ac$, $a \neq 0$ implies $b = c$ and the equation $ba = ca$, $a \neq 0$ implies $b = c$ in $A$.*

**Definition 2.8.** A *division ring* (also called a *skew field*) is a ring $A$ such that for any $a \in A$, $a \neq 0$, there exists $b \in A$ such that $ab = ba = 1$. Equivalently, a division ring is a ring where the nonzero elements $A \setminus \{0\}$ form a group with respect to multiplication.

**Proposition 2.9.** *A division ring is a domain.*

Proof: If for any $a \neq 0$ in $A$, there exists $x \in A$ such that $ax = 1$, then if $a$ is a (right) zero divisor, we have a nonzero $b \in A$ such that $ba = 0$, and $bax = b1 = b = 0$, a contradiction. Similarly for the left zero divisors.

**Definition 2.10.** A commutative division ring is called a *field*.

| | | | | |
|---|---|---|---|---|
| Division rings | $\subset$ | Domains | $\subset$ | Rings |
| Fields = Commutative division rings | $\subset$ | Integral domains | $\subset$ | Commutative rings. |

**Corollary 2.11.** *The ring $A = \mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n = p$ is a prime.*

# 3 Ideals

**Definition 3.1.** Let $A$ be a ring. A *left ideal* is a subset $I \subset A$ such that (1) $I \subset A$ is a subgroup with respect to addition, and (2) $ax \in I \;\; \forall x \in I, a \in A$. Similarly, $J \subset A$ is a *right ideal* in $A$ if (1) $J$ is a subgroup with respect to addition and (2) $ya \in J \;\; \forall y \in J, a \in A$.

**Definition 3.2.** If $I \subset A$ is a left and a right ideal, it is called a *two-sided ideal*, or simply an *ideal* in $A$.

**Remark 3.3.** (1) In a commutative ring every left or right ideal is a two-sided ideal. (2) The subsets $\{0\} \subset A$, $A \subset A$ are ideals in any ring $A$. A *proper ideal* $I \subset A$ is such that $I \neq A$. (3) For any ideal $I \subset A$, $0 \in I$.

From now on we will consider only commutative rings

**Proposition 3.4.** *Let $A$ be a commutative ring. Here are some properties of the ideals.*

*(a) If $I \subset A$ is an ideal and $1 \in I$, then $I = A$.*

*(b) If $I, J \subset A$ are ideals, then $I \cap J \subset A$ is also an ideal*

*(c) If $I, J \subset A$ are ideals, the subset $I \cup J \subset A$ is not necessarily an ideal.*

*(d) If $I, J \subset A$ are ideals, then the set $\{x + y\}$, $x \in I$, $y \in J$ is an ideal denoted by $I + J$.*

*(e) If $I, J \subset A$ are ideals, then the set $\{\sum_{i=1}^{k} x_i y_i\}$, $x_i \in I$, $y_i \in J$ is an ideal denoted by $I \cdot J$.*

**Definition 3.5.** Let $S \subset A$ be an arbitrary subset in a ring $A$. Consider the intersection of all ideals in $A$ containing $S$. This is an *ideal generated by the set $S$*, denoted by $(S) \subset A$. Let $A$ be a commutative ring, and $S = \{s_i\}_{i \in T}$, where $T$ is a finite or infinite set of indices. Then $(S) = \{\sum_i a_i s_i\}_{a_i \in A}$.

**Theorem 3.6.** *Let $A$ be a commutative ring. Then $A$ is a field if and only if the only ideals in $A$ are $\{0\}$ and $A$.*

**Definition 3.7.** An ideal $I \subset A$ is called *principal* if it is generated by a single element in $x \in A$: $I = (x)$.

**Definition 3.8.** Let $A$ be a commutative ring. An ideal $I \subset A$ is called *prime* if for any $a, b \in A$, if $ab \in I$, then at least one of $a$ and $b$ is in $I$.

**Definition 3.9.** Let $A$ be a commutative ring. A proper ideal $I \subset A$ is called *maximal* if there exists no other proper ideal $J \subset A$ such that $I \subset J$ is a proper subset.

# 4 Equivalence and congruence relations. Quotient ring.

**Definition 4.1.** A relation $x \sim y$ on a set $E$ is an *equivalence relation* if it satisfies the axioms:
1. $x \sim x$ for any $x \in E$ (reflexivity)
2. $x \sim y \implies y \sim x$ (symmetry)
3. $x \sim y$ and $y \sim z \implies x \sim z$ (transitivity) .

**Definition 4.2.** An *equivalence class* of element $x \in E$ is the subset $\bar{x} = \{y \in E \, : \, x \sim y\}$.

**Remark 4.3.** The transitivity of an equivalence relation implies that if $x \neq y \in E$, then $\bar{x} = \bar{y}$, or $\bar{x} \cap \bar{y} = \emptyset$. The set of equivalence classes $E/\sim$ is called the *quotient set* with respect to $\sim$.

**Definition 4.4.** Let $A$ be a commutative ring. An equivalence relation $\sim$ on $A$ is a *congruence relation* if $a \sim b, c \sim d$ implies $a + c \sim b + d$ and $ac \sim bd$.

**Proposition 4.5.** *Let $A$ be a commutative ring and $\sim$ a congruence relation such that $0 \nsim 1$. The set of congruence classes $A/\sim$ has a structure of a commutative ring*[1].

**Proposition 4.6.** *Let $A$ be a commutative ring.*
*(1) If $I \subset A$ is an ideal, then the relation $a \sim b \Leftrightarrow (a - b) \in I$ is a congruence relation in $A$.*
*(2) If $\sim$ is a congruence relation in $A$, then the set $I = \{a \in A, \; a \sim 0\}$ is an ideal in $A$.*

**Definition 4.7.** An ideal $I \subset A$ defines a quotient ring $A/I$ whose elements are the congruence classes modulo the ideal $I$. An ideal in a commutative ring plays the same role as a normal group in a group.

[1] If $1 \sim 0$, the obtained structure $A/\sim$ satisfies all the axioms of a ring, except that it does not have a unit, and is sometimes called *rng*.

## 5 The ring $\mathbb{Z}$: ideals and quotients.

**Definition 5.1.** A commutative ring $A$ is a principal ideal ring if every ideal in $A$ is principal. An integral domain where each ideal is principal is called a principal ideal domain.

**Proposition 5.2.** *The ring $\mathbb{Z}$ of integers is a principal ideal domain.*

**Corollary 5.3.** *Let $I \subset \mathbb{Z}$ be an ideal generated by integers $\{a_1, a_2, \dots a_n\}$. Then $I = (d) \subset \mathbb{Z}$, where $d = \gcd(a_1, a_2, \dots a_n)$.*

## 6 Homomorphisms and characteristic of a ring. Direct products of rings

**Definition 6.1.** A map $f : A \to B$ between rings $A$ and $B$ is a ring homomorphism if it respects the ring operations, namely $f(a+b) = f(a) + f(b)$ (this implies $f(0_A) = 0_B$), $f(ab) = f(a)f(b)$ for any $a, b \in A$, and $f(1_A) = 1_B$.

**Proposition 6.2.** *If $f : A \to B$ is a homomorphism of commutative rings, then $\ker(f) = \{a \in A \ : f(a) = 0\}$ is an ideal in $A$, and $\operatorname{im}(f) \subset B$ is a subring in $B$ (a subring is an additive subgroup of a ring containing $1$ and closed with respect to the multiplication).*

**Proposition 6.3.** *Let $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ a ring homomorphism. Then $m|n$, and $f([a]_n) = [a]_m$.*

**Proposition 6.4.** *For any ring $A$ there is a unique homomorphism $\tau : \mathbb{Z} \to A$. Then $\ker(\tau) = \{0\}$, or $\ker(\tau) = (d)$ for a positive integer $d \in \mathbb{Z}$.*

**Definition 6.5.** Let $A$ be a ring and $\tau : \mathbb{Z} \to A$ the unique ring homomorphism. Then the characteristic $c_A$ of the ring $A$ is defined as follows:

$$\begin{aligned} c_A &= 0, \quad \text{if} \quad \ker(\tau) = \{0\}, \\ c_A &= d, \quad \text{if} \quad \ker(\tau) = (d). \end{aligned}$$

**Proposition 6.6.** *Let $A$ be a ring such that the characteristic of $A$ is $n = mk \in \mathbb{Z}^+$, where $m, k \geq 2$ are integers. Then $A$ has a nontrivial zero divisor.*

**Corollary 6.7.** *The characteristic of a field is either $0$, or a prime number $p$.*

**Corollary 6.8.** *The converse to Corollary 6.7 is false: there exists a ring with characteristic $p$ that is not a field.*

**Definition 6.9.** Let $A$ and $B$ be two rings. We define the direct product $A \times B$ as the set of pairs $\{(a, b), a \in A, b \in B\}$ with coordinate-wise addition and multiplication. In particular, $1_{A\times B} = (1_A, 1_B)$ and $0_{A\times B} = (0_A, 0_B)$.

If $A$ and $B$ are two commutative rings, and $c_A \neq 0$, $c_B \neq 0$, then $c_{A\times B} = \operatorname{lcm}(c_A, c_B)$.

## 7 Chinese remainder theorem for integers

Recall that an ideal $I \subset A$ in a commutative ring $A$ defines a quotient ring $A/I$ (see Definition 4.7).

**Theorem 7.1.** *Let $I, J$ be two ideals in a commutative ring $A$, such that $I + J = A$. Then there is a ring isomorphism*

$$f : A/(I \cap J) \to A/I \times A/J,$$

*given by the diagonal map $f : \bar{x}_{I\cap J} \to (\bar{x}_I, \bar{x}_J)$.*

**Corollary 7.2.** *Let $m, n \in Z$ be coprime numbers. Then for any $a_1, a_2 \in \mathbb{Z}$ there exists $a \in \mathbb{Z}$ such that $a \equiv a_1 \pmod m$ and $a \equiv a_2 \pmod n$. The set of solutions for $a$ is given by $a + mn\mathbb{Z}$.*

**Theorem 7.3.** *Let $d_1, d_2, \dots d_n$ be integers such that $\gcd(d_i, d_j) = 1$ for any $i \neq j$. Let $d = d_1 d_2 \dots d_n$. Then we have a ring isomorphism*

$$f : \mathbb{Z}/(d) \to \mathbb{Z}/(d_1) \times \mathbb{Z}/(d_2) \times \dots \times \mathbb{Z}/(d_n),$$

*given by $f([a]_d) = ([a]_{d_1}, [a]_{d_2}, \dots [a]_{d_n})$.*

**Corollary 7.4.** *Let $d_1 \dots d_r \in \mathbb{Z}$ be pairwise coprime numbers, meaning that $\gcd(d_i, d_j) = 1$ for any pair of indices $1 \leq i \neq j \leq r$. Then for any $a_1, a_2, \dots a_r \in \mathbb{Z}$ there exists $a \in \mathbb{Z}$ such that*

$$\begin{aligned} &a \equiv a_1 \pmod{d_1}, \\ &a \equiv a_2 \pmod{d_2}, \\ &\dots \\ &a \equiv a_r \pmod{d_r}. \end{aligned}$$

*Let $d = d_1 d_2 \dots d_r$. The set of all solutions of the given congruences is given by $a + d\mathbb{Z}$.*

**Remark 7.5.** The proof of Theorem 10.1 provides a method to solve systems of congruences: suppose you have to solve a system of congruences modulo $d_1, d_2, \ldots d_r$ where the elements $d_1, d_2, \ldots d_r$ are pairwise mutually prime. Solve the first pair of congruences modulo $d_1$ and $d_2$ first, then the obtained result gives a new congruence modulo the product $d_1 d_2$. The product $d_1 d_2$ is coprime to $d_3$. Solve these two congruences, obtaining a congruence modulo $d_1 d_2 d_3$. The product $d_1 d_2 d_3$ is coprime to $d_4$, so you can again solve the pair of congruences, and so on until you solve the last congruence.

In fact we can make a method even more explicit. Suppose we have a system of congruences $x \equiv a_i \pmod{d_i}$ for $i = 1...k$. Consider $d = d_1 d_2 \ldots d_k$ and set $D_i = d/d_i$. Then we have $\gcd(d_i, D_i) = 1$. Therefore, by Bezout's identity there exist integers $x_i$ and $y_i$ such that $D_i x_i + d_i y_i = 1$. Then $x = \sum_{i=1}^k a_i D_i x_i$. Indeed, $x \equiv a_i D_i x_i \pmod{d_i}$, because $d_i | D_j$ for $j \neq i$. Therefore, $x \equiv a_i(1 - d_i y_i) \pmod{d_i} \equiv a_i \mod (d_i)$. The solution is determined modulo $D$.

**Remark 7.6.** Note that if the rings $A$ and $B$ are isomorphic, then their groups of units are also isomorphic: $A^* \simeq B^*$. This follows from the fact that the ring isomorphism respects the multiplication in both rings.

**Corollary 7.7.** *Let $n, m \in \mathbb{Z}$ be such that $\gcd(n, m) = 1$. Then we have for the Euler's totient function:*

$$\varphi(nm) = \varphi(n) \cdot \varphi(m).$$

# 8 Polynomials in one variable with coefficients in a commutative ring.

**Definition 8.1.** Let $A$ be an commutative ring, and consider the ring of polynomials in one variable $A[x]$. Then $A[x] = \{a_0 + a_1 x + \ldots + a_n x^n\}$, where $n \in \mathbb{N}$ and $a_0, a_1, \ldots a_n$ are elements of $A$. Equivalently, $A[x] = \{(a_0, a_1, \ldots)\}_{a_i \in A}$ such that $a_i = 0$ for large enough $i \in \mathbb{N}$. Clearly $A[x]$ is a commutative ring with respect to the usual addition and multiplication of polynomials.

**Definition 8.2.** If $f(x) \in A[x]$ is nonzero, then the degree of the polynomial $f(x) = a_0 + a_1 x + \ldots$ is the largest integer $n$ such that $a_n \neq 0$, $\deg(f(x)) = n$. The element $a_n \in A$ is called the dominant coefficient, and $a_0 \in A$ the constant term. If $f(x) = 0$, we define $\deg(0) = -\infty$.

**Proposition 8.3.** *In the ring $A[x]$ we have:*

*(a)* $\deg(f(x) + g(x)) \leq \max(\deg(f(x)), \deg(g(x)))$

*(b) If $A$ is an integral domain, then* $\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x))$.

**Theorem 8.4.** *Let $A$ be an integral domain. The ring of polynomials $A[x]$ is also an integral domain. The invertible elements in $A[x]$ are the invertible elements in $A$.*

**Theorem 8.5.** *Let $F$ be a field, and $f(x), d(x)$ polynomials in $F[x]$, such that $\deg(d(x)) \geq 1$. There exist polynomials $q(x), r(x) \in F[x]$ such that $f(x) = q(x)d(x) + r(x)$, and either $r(x) = 0$, or $\deg(r(x)) < \deg(d(x))$.*

# 9 Euclidean domains and principal ideal domains

**Definition 9.1.** A commutative ring $A$ is a Euclidean domain if
(1) $A$ is an integral domain, and
(2) there exists a function $\nu : A \setminus \{0\} \to \mathbb{N}$ such that for all $a, b \in A$, $b \neq 0$, there exists $q, r \in A$ such that $a = qb + r$ and either $r = 0$, or $\nu(r) < \nu(b)$.

**Corollary 9.2.** *If $F$ is a field, then the ring of polynomials $F[x]$ is a Euclidean domain.*

**Theorem 9.3.** *A Euclidean domain is a principal ideal domain.*

**Corollary 9.4.** *Let $F$ be a field. The ring $F[x]$ is a principal ideal domain, meaning that any ideal in $F[x]$ is generated by a single polynomial.*

**Definition 9.5.** Let $A$ be a commutative ring. For $a, b \in A$ we say that *a* divides *b*, if there exists $c \in A$ such that $b = ac$. In this case we can write, just like for the integers, $a|b$.

**Definition 9.6.** Let $A$ be an integral domain. The elements $a, b \in A$ are associates if $b = au$ for a unit $u \in A^*$ (equivalently, $a = bv$ for a unit $v \in A^*$).

**Definition 9.7.** Let $A$ be an integral domain. Let $a, b \in A$. We say that $c \in A$ is a common divisor of $a$ and $b$ if $c|a$ and $c|b$. We say that $d \in A$ is a greatest common divisor of $a$ and $b$ if $d|a, d|b$, and if $c$ is a common divisor of $a$ and $b$, then $c|d$. We denote $d = \mathrm{gdc}(a, b)$. We say that $l \in A$ is a least common multiple of $a$ and $b$ if $a|l$, $b|l$, and if $a|t$ and $b|t$, then $l|t$. We denote $l = \mathrm{lcm}(a, b)$.

**Proposition 9.8.** *Let $A$ be an integral domain. If $d_1, d_2$ are greatest common divisors of $a, b \in A$, then $d_1$ and $d_2$ are associates. If $l_1, l_2$ are least common multiples of $a, b \in A$, then $l_1$ and $l_2$ are associates.*

**Proposition 9.9.** *Properties of the Euclidean domains.*

(a) *Euclidean algorithm works in a Euclidean domain: If $a, b \in E$, $b \neq 0$, then there exist $q, r \in E$ such that $a = qb + r$ and either $r = 0$ (then $b = \gcd(a, b)$), or $\nu(r) < \nu(b)$. Repeat with $b = q_2 r + r_2$, with $\nu(r_2) < \nu(r)$, and so on. The process terminates because the function $\nu : E \to \mathbb{N}$ is strictly decreasing. We have $r_{n-1} = q_n r_n$. Then the greatest common divisor $r_n = \gcd(a, b)$.*

(b) *Bezout's theorem: If $d = \gcd(a, b)$, then there exist $x, y \in E$ such that $xa + yb = d$. It follows that the ideal $(a) + (b) = (d) \subset E$.*

(c) *If $a, b \in E$ are such that $\gcd(a, b) = 1$, and $a|bc$ for $c \in E$, then $a|c$. In particular, if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.*

(d) *If $a, b \in E$ are such that $\gcd(a, b) = 1$, and $a|c$ and $b|c$ for an element $c \in E$, then $ab|c$. In particular, if $\gcd(a, b) = 1$, then $\mathrm{lcm}(a, b) = ab$.*

(e) *The ideal $(a) \cap (b) = (m) \subset E$, where $m = \mathrm{lcm}(a, b)$.*

**Remark 9.10.** Let $f(x), g(x) \in F[x]$, so that the Euclidean division works. If $\gcd(f(x), g(x)) = d_1(x)$ and $\gcd(f(x), g(x)) = d_2(x)$, then by Proposition 9.8 $d_1(x) = ud_2(x)$, where $u \in \mathbb{R}[x]$ is a unit, which implies $u \neq 0, u \in \mathbb{R}$. Then we can choose a unique *monic* polynomial $d(x) = \gcd(f(x), g(x))$, such that the dominant coefficient of $d(x)$ is 1. Note that the ideals generated by the associates are the same: $(d_1) = (d_2) = (d)$.

Conclusions: Let E be a Euclidean domain.

1. E is a principal ideal domain.
2. If $a, b \in E$ two nonzero elements, then the ideals $(a) \cap (b) = (\mathrm{lcm}(a, b)) \subset E$ and $(a) + (b) = (\gcd(a, b)) \subset E$.
3. $\gcd(a, b)$ and $\mathrm{lcm}(a, b)$ are determined up to a multiplication by a unit in $E$. Associate elements generate equal ideals in $E$.

## 10 Chinese remainder theorem for a Euclidean domain.

Let $A$ be a Euclidean domain, so that for nonzero $a, b \in E$ there exists $\gcd(a, b) \in E$ that is well defined up to a multiplication by a unit. In addition, $A$ is a principal ideal domain so that any ideal is generated by a single element.

**Theorem 10.1.** *Let $A$ be a Euclidean domain, and $m_1, m_2, \ldots m_r$ elements such that $\gcd(m_i, m_j) = 1$ for any two indices $1 \leq i \neq j \leq r$. Let $m = m_1 m_2 \ldots m_r$. Then the map*

$$f : A/(m) \to A/(m_1) \times A/(m_2) \times \ldots \times A/(m_r),$$

*given by $f(\bar{x}_{(m)} = (\bar{x}_{(m_1)}, \bar{x}_{(m_2)}, \ldots \bar{x}_{(m_r)})$ is an isomorphism of rings.*

**Corollary 10.2.** *(Chinese remainder theorem for polynomial rings). Let $F$ be a field, $\{f_1(x), f_2(x), \ldots f_r(x)\}$ polynomials in $F[x]$ such that $\gcd(f_i, f_j) = 1$. Then the exist a ring isomorphism*

$$\Phi : F[x]/(f_1(x) \cdot f_2(x) \cdot \cdot f_r(x)) \simeq F[x]/(f_1(x)) \times F[x]/(f_2(x)) \times \ldots \times F[x]/(f_r(x)).$$

## 11 Irreducible elements in Euclidean domains.

**Definition 11.1.** Let $A$ be an integral domain. The element $c \in A$ is irreducible if $c$ is not a unit in $A$ ($c$ is not invertible in $A$), $c \neq 0$, and if $c = ab$ for $a, b \in A$, then $a$ or $b$ is a unit.

**Example 11.2.** In the ring $\mathbb{Z}$ the units are $\{\pm 1\}$ and the irreducible elements are $\{\pm p\}$, where $p$ are the prime numbers.

Recall that an ideal $I \subset A$ is maximal if there is no ideal $J \subset A$ such that $I \subsetneq J \subsetneq A$.

**Theorem 11.3.** *Let $A$ be a PID. Then $p \in A$ an irreducible element if and only if $p \neq 0$ and the ideal $(p) \subset A$ is maximal.*

**Proposition 11.4.** *Let $A$ be a Euclidean domain and $I = (a)$ a nontrivial ideal: $I \neq \{0\}$ and $I \neq A$. Then*

*(a) $\bar{b}$ is a unit in $A/I$ if and only if $\gcd(a, b) = 1$.*

*(b) $\bar{b}$ is a nontrivial zero divisor in $A/I$ if and only if $b \notin I$ and $\gcd(a, b) \neq 1$.*

*(c) $A/I$ is a field for $I = (a)$ if and only if $a \in A$ is irreducible.*

**Corollary 11.5.** *Let $F$ be a field and consider the ring $F[x]$ of polynomials in one variable with coefficients in $F$. Let $f(x) \in F[x]$ be a nonzero polynomial. Then $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible in $F[x]$.*

### Conclusions.

1. We have the following inclusions :
   Fields $\subset$ Euclidean domains $\subset$ Principal ideal domains $\subset$ Integral domains $\subset$ Commutative rings.

2. Fields, $\mathbb{Z}$, $F[x]$ for $F$ a field, Gaussian integers $\mathbb{Z}[i]$ are examples of Euclidean domains (and of PIDs).

3. $\mathbb{Z}[x]$, $F[x, y]$, where $F$ a field are integral domains but not PIDs.

4. The rings $\mathbb{Z}/n\mathbb{Z}$, where $n$ is not a prime, and $(\mathbb{Z}/n\mathbb{Z})[x]$ are not integral domains.

## 12 Quotients of polynomial rings

Let us recall what we know about the ring $F[x]$, where $F$ is a field.

**Remark 12.1.** Properties of the polynomial ring $F[x]$, where $F$ is a field.

1. The ring $F[x]$ is a Euclidean domain, in particular it is a PID: any ideal in $F[x]$ is generated by a single element.

2. An ideal generated by $f(x)$ is maximal if and only if $f(x)$ is irreducible. A quotient ring $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible in $F[x]$. (Corollary 11.5).

3. For any two polynomials $f(x), g(x)$, such that $\deg(f(x)) \geq 1$ and $\deg(g(x)) \geq 1$, there exist $\gcd(f(x), g(x))$ and $\mathrm{lcm}(f(x), g(x))$, unique up to multiplication by units. They generate the ideals $(f(x))+(g(x)) = (\gcd(f(x), g(x)))$ and $(f(x)) \cap (g(x)) = (\mathrm{lcm}(f(x), g(x)))$.

4. The characteristic of $F[x]$ is equal to the characteristic of $F$, which can be $0$ or a prime number. If $f(x)$ is irreducible (in particular, $\deg(f) \geq 1$), then the characteristic of $F[x]/(f(x))$ equals that of $F$.

**Proposition 12.2.** *Let $F$ be a field.*

1. *Any polynomial of degree 1 is irreducible in $F[x]$.*

2. *A polynomial of degree 2 or 3 is irreducible if and only if it has no root in $F$.*

**Proposition 12.3.** *Suppose that $\alpha = \frac{r}{s} \in \mathbb{Q}$ is a root of the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. Then $s | a_n$ and $r | a_0$. In particular, any rational root of a monic polynomial with integer coefficients is an integer.*

**Proposition 12.4.** *(Eisenstein's criterion). Let $f(x) = a_0 + a_1 x + \ldots a_{n-1} x^{n-1} + a_n x^n \in \mathbb{Z}[x]$ be a polynomial with integer coefficients, such that $\gcd(a_0, a_1, \ldots a_n) = 1$. Suppose that there exists a prime $p \in \mathbb{Z}$ such that $p | a_i$, $0 \leq i \leq n-1$, $p$ does not divide $a_n$, and $p^2$ does not divide $a_0$. Then $f(x)$ is irreducible over $\mathbb{Q}[x]$ (and also over $\mathbb{Z}[x]$).*

**Proposition 12.5.** *Let $F$ be a field, and $f(x) \in F[x]$ an irreducible polynomial of degree $n \geq 1$. The ring $K = F[x]/(f(x))$ is a field, such that any element of $K$ can be written uniquely in the form*

$$a_0 \overline{1} + a_1 \overline{x} + \ldots + a_{n-1} \overline{x^{n-1}},$$

*where $a_i \in F$ and $\overline{x^i}$ is the congruence class $x^i + (f(x))$.*

**Corollary 12.6.** *If $F$ is a finite field of $q$ elements, and $f(x) \in F[x]$ an irreducible polynomial of degree $n \geq 1$, then the field $F[x]/(f(x))$ has exactly $q^n$ elements.*

## 13 Finite fields

Recall that the characteristic of a field can be either 0 or a prime number $p$.

**Proposition 13.1.** *Let $\mathbb{F}_p$ denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$.*

*(a) Let $K$ be a field of $p^n$ elements for some $n \in \mathbb{N}^+$. Then the characteristic of $K$ is $p$.*

*(b) Any field with $p$ elements is isomorphic to $\mathbb{F}_p$.*

*(c) Let $K$ be a field of characteristic $p$. There exists a subfield in $K$ isomorphic to $\mathbb{F}_p$.*

*(d) Let $K$ be a finite field of characteristic $p$. Then it has $p^n$ elements for some $n \in \mathbb{N}^+$.*

**Proposition 13.2.** *Let $F$ be a field and $f(x) \in F[x]$ a polynomial. Then there exists a field $K \supset F$ that contains all the roots of $f$.*

**Proposition 13.3.** *The group of units of a finite field $K$ is cyclic.*

**Theorem 13.4.** *Let $p$ be a prime and $n \in \mathbb{N}$, $n > 1$. Then there exists a unique field $K$ with $|K| = p^n$ and an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ such that $\mathbb{F}_p[x]/(f(x)) \simeq K$. If $g(x) \in \mathbb{F}_p[x]$ is another irreducible polynomial of degree $n$ over $\mathbb{F}_p$, then $K \simeq \mathbb{F}_p[x]/(f(x)) \simeq \mathbb{F}_p[x]/(g(x))$.*

**Corollary 13.5.** *For any $n \in \mathbb{N}^+$ and any prime $p$ there is an irreducible polynomial $f(x)$ of degree $n$ over $\mathbb{F}_p$.*

### Conclusions.

1. For any prime $p$, any $n \in \mathbb{N}^*$ there exist a unique finite field $\mathbb{F}_{p^n}$ of $p^n$ elements, with $\mathrm{char}(\mathbb{F}_{p^n}) = p$.
2. For $n = 1$, this finite field is isomorphic to $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$.
3. For $n > 1$, this unique field can be constructed as a quotient

$$\mathbb{F}_{p^n} \simeq \mathbb{F}_p[x]/(f(x)),$$

where $f(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree $n$.