Fall 2022

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 $ab = ba$ $\forall a, b \in A$.

Example 1.3. The number sets $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ are rings with respect to the usual addition and multiplication. Also, the set $\mathbb{Z}[\sqrt{2}] = \{m + \sqrt{2}n\}_{m,n\in\mathbb{Z}}$ is a commutative ring: $(m_1 + \sqrt{2}n_1)(m_2 + \sqrt{2}n_2) = m_1m_2 + 2n_1n_2 + \sqrt{2}(n_1m_2 + m_1n_2)$ and $(m_1 + \sqrt{2}n_1) + (m_2 + \sqrt{2}n_2) = m_1 + m_2 + \sqrt{2}(n_1 + n_2)$.

Example 1.4. The set of all $n \times n$ matrices $M_n(\mathbb{Z})$ with integer coefficients is a ring with respect to matrix addition and multiplication. Indeed, adding or multiplying two matrices with integer entries gives a matrix with integer entries. The neutral element for addition is the zero matrix, and for multiplication the identity matrix with units on the diagonal and zeros in other positions. The multiplication is non-commutative: in general $M_1 \cdot M_2 \neq M_2 \cdot M_1$. Note not all elements have a multiplicative inverse in this ring, because even if the matrix is nonsingular, the inverse of a matrix with integer coefficients does not necessarily have integer coefficients. We emphasize that the existence of a multiplicative inverse is not required in the definition of a ring.

Example 1.5. Another important example of a ring is the ring of polynomials in one variable with real or complex coefficients, $\mathbb{R}[x]$ or $\mathbb{C}[x]$. This is a commutative ring with elements of the form $a_0 + a_1 + \cdot + a_k x^k$. The neutral elements for addition and multiplication are respectively the constant polynomials 0 and 1.

Remark 1.6. In any ring, the operation of multiplication by an integer number is well defined. Indeed, let A be a ring and $a \in A$ an element. For any $n \in \mathbb{N}$ we define na to be the sum $a + a + a + \ldots a \in A$ (where a is added n times). Then $(-n)a = -na$ and the following equalities are satisfied:

$$(n+m)a = na + ma, \qquad n(a+b) = na + nb, \qquad (nm)a = n(ma) \qquad \forall n, m \in \mathbb{Z},\ \forall a, b \in A.$$

Proposition 1.7. *Let A be a commutative ring. Then for any $a, b \in A$ and $n \in \mathbb{N}^*$ we have the binomial formula*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Proof: by induction.

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. 1. The element 0 is a left and right zero divisor in any ring.

2. 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*.

Example 2.5. The matrix ring $M_n(\mathbb{Z})$ is not a domain. Here is an example of two nonzero matrices whose product is zero:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Remark 2.6. In the matrix ring $M_n(\mathbb{R})$ a left zero divisor is a right zero divisor, and vice versa.

Definition 2.7. A commutative ring whose only zero divisor is 0 is called an *integral domain*.

Example 2.8. The rings $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ are integral domains.

Example 2.9. Let $n \geq 2$ be an integer. Consider the set of congruence classes $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n. We already know that this is a group with respect to addition, isomorphic to the cyclic group C_n. Multiplication is also well defined in $\mathbb{Z}/n\mathbb{Z}$ (and leads to the definition of the multiplicative group of units $(\mathbb{Z}/n\mathbb{Z})^*, \cdot)$). One can easily check that the whole set $\mathbb{Z}/n\mathbb{Z}$ with the addition and multiplication is a commutative ring with $[0]_n$ and $[1]_n$ the neutral elements with respect to the addition and multiplication. The invertible elements (units) in $\mathbb{Z}/n\mathbb{Z}$ are the precisely the elements that are not the zero divisors.

Corollary 2.10. *The ring $A = \mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if $n = p$ is a prime.*

Proof: An element $[m]_n \in \mathbb{Z}/n\mathbb{Z}$ is a zero divisor if and only if $\gcd(m, n) = d > 1$. On the other hand, if $\gcd(n, m) = 1$, then by Bezout's theorem, $mx + ny = 1$ for some $x, y \in \mathbb{Z}$. Then $[m]_n[x]_n = [1]_n$, and $[m]_n$ is invertible. The number of invertible elements in $\mathbb{Z}/n\mathbb{Z}$ equals to $\phi(n)$, the Euler's totient function of n. It follows that all nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ are invertible, and consequently not zero divisors, if and only if $n = p$ is a prime.

Example 2.11. Consider the set $C^0([0, 1])$ of continuous functions $f : [0, 1] \to \mathbb{R}$. It is easy to check that $C^0([0, 1])$ is a commutative ring with respect to pointwise addition and multiplication of functions. It is not an integral domain, because a product of two functions with nonzero values on non-intersecting subintervals gives a constant zero function.

Proposition 2.12. *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.*

Proof: Suppose $ax = 0$ for some nonzero $a \neq 0$, $x \neq 0$. Then $ax = a0$, and if the cancelation law applies, then $x = 0$, a contradiction. Conversely, suppose A is a domain and $ab = ac$ with $a \neq 0$. Then $a(b - c) = 0$, and since A contains no zero divisor, this implies $b - c = 0$ and $b = c$.

Definition 2.13. 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.

Example 2.14. $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ are division rings. But $\mathbb{Z}$ is not a division ring: the equation $3 \cdot x = 1$ has no solution in $\mathbb{Z}$.

Example 2.15. The quaternions provide an example of a non-commutative division ring:

$$H = \{a + ib + jc + kd\}_{a,b,c,d \in \mathbb{R}}.$$

The relations are $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, $i^2 = j^2 = k^2 = -1$. Check that every nonzero element in H is invertible.

Proposition 2.16. *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 2.17. A commutative division ring is called a *field*.

Remark 2.18. Here we arrive at a familiar conclusion that $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field.

We have the following inclusions:
Division rings $\subset$ Domains $\subset$ Rings
Fields = Commutative division rings $\subset$ Integral domains $\subset$ Commutative rings.

Corollary 2.19. *The ring $A = \mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n = p$ is a prime (see the proof of Corollary 2.10).*

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 $I \subset A$, $0 \in I$.

Example 3.4. Let $M_n(\mathbb{R})$ be the ring of $n \times n$ real matrices. Then matrices with the first row of zeros form a right ideal. The matrices with the first column of zeros form a left ideal.

Example 3.5. The subsets $d\mathbb{Z} \subset \mathbb{Z}$ of multiples of a given number $d \in \mathbb{Z}$ are ideals in the ring $\mathbb{Z}$.

Example 3.6. The functions $f \in C^0([0,1])$ such that $f(\frac{1}{2}) = 0$ form an ideal in the ring $C^0([0,1])$ of continuous functions $f : [0,1] \to \mathbb{R}$.

From now on we will consider only commutative rings

Proposition 3.7. *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 $I \cdot J$.

Proof:

(a) If $1 \in I$, then $a = a \cdot 1 \in I$ for any $a \in A$.

(b) Let $x \in I \cap J$, then $ax \in I \cap J$ for any $a \in A$, and $I \cap J$ is a subgroup with respect to addition.

(c) See counter-example 3.8 below.

(d) Clearly the set $\{x + y\}, x \in I, y \in J$ is a subgroup with respect to addition. Also, we have $a(x + y) = ax + ay$, where $ax \in I$ and $ay \in J$, so $I + J$ is an ideal.

(e) Clearly the set $\{\sum_{i=1}^{k} x_i y_i\}$, $x_i \in I$, $y_i \in J$ is a subgroup with respect to addition. Also, we have $a \sum_{i=1}^{k} x_i y_i = \sum_{i=1}^{k} (ax_i) y_i = \sum_{i=1}^{k} \tilde{x_i} y_i$, where $\tilde{x_i} \in I$ for all $i, 0 \leq i \leq k$. Therefore the subset $I \cdot J \subset A$ is an ideal.

Example 3.8. Consider the ideals $I = 3\mathbb{Z} \in \mathbb{Z}$ and $J = 5\mathbb{Z} \in \mathbb{Z}$. Then $I \cap J = 15\mathbb{Z} \subset \mathbb{Z}$, while $I \cup J = \{0, \pm 3, \pm 5 \pm 6, \pm 9, \pm 10, \ldots\}$ is not an ideal: this set is not closed with respect to addition, as $3 + 5 = 8 \notin I \cup J$. The ideal $I + J$ contains $1 = 6 - 5$, and therefore $I + J = \mathbb{Z}$. The ideal $I \cdot J = 15\mathbb{Z}$.

Exercise 3.9. Let $I = 12\mathbb{Z} \in \mathbb{Z}$ and $J = 15\mathbb{Z} \in \mathbb{Z}$. Then $I \cap J = 60\mathbb{Z} = \text{lcm}(12, 15)\mathbb{Z}$, $I + J = 3\mathbb{Z} = \gcd(12, 15)\mathbb{Z}$, and $I \cdot J = 180\mathbb{Z} = 12 \cdot 15\mathbb{Z}$.

Exercise 3.10. If I, J are two ideals in a commutative ring A, then we have

$$I \cdot J \subset I \cap J \subset I \subset I + J, \qquad I \cdot J \subset I \cap J \subset J \subset I + J.$$

Definition 3.11. 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 3.12. *Let A be a commutative ring. Then A is a field if and only if the only ideals in A are $\{0\}$ and A.*

Proof: (1) Suppose that A is a field, and let $a \in I$ be a a nonzero element in an ideal $I \subset A$. Then $a^{-1} \in A$, which implies $a^{-1}a = 1 \in I$. Therefore, $I = A$. (2) Now suppose that $a \in A$ be a nonzero element and consider $I = (a)$, the ideal generated by a. Since $a \neq 0$, we have $I \neq \{0\}$, and therefore $I = A$, and $1 \in I$. Then $1 = ab$ for some $b \in A$, and therefore a is invertible in A, and so A is a field.

Example 3.13. The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ for a prime p are fields.

Definition 3.14. An ideal $I \subset A$ is called *principal* if it is generated by a single element in $x \in A$: $I = (x)$.

Example 3.15. The ideal $(n) \subset \mathbb{Z}$ of multiples of an integer number n is a principal ideal. Note that $(0) = \{0\}$ and $(1) = \mathbb{Z}$. We will see later that all ideals in $\mathbb{Z}$ are of the form $(n) \subset \mathbb{Z}$.

Definition 3.16. 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 3.17. 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.

Exercise 3.18. Consider the ideals of the form $d\mathbb{Z} \subset \mathbb{Z}$, where $d \in \mathbb{N}$. Then an ideal is prime if and only if $d = p$ is a prime number. Also, an ideal is maximal if and only if $d = p$ is a prime.

Example 3.19. Let $I = ((x+5)) \subset \mathbb{R}[x]$ be the ideal of polynomials divisible by $(x+5)$, and $J = ((x^2-1)) \subset \mathbb{R}[x]$ the ideal of polynomials divisible by (x^2-1). Then the ideal $I \cap J = I \cdot J$ is spanned by the polynomials divisible by the product $(x+5)(x^2-1)$, and the ideal $I + J = \mathbb{R}[x]$, because $\frac{1}{24}(x^2-1) - \frac{1}{24}(x-5)(x+5) = 1 \in I + J$.

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) .

Example 4.2. Let $E = \mathbb{R}^n \setminus \{0\}$. The relation $v \sim u \Leftrightarrow \exists \lambda \in \mathbb{R}^* : v = \lambda u$ is an equivalence relation in E.

Definition 4.3. An *equivalence class* of element $x \in E$ is the subset $\bar{x} = \{y \in E \,:\, x \sim y\}$.

Remark 4.4. 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 $\sim$.

Example 4.5. In the example 4.2 the equivalence classes are the lines passing through the origin. The quotient set is the real projective space $\mathbb{RP}^n$, the set of all lines in $\mathbb{R}^n$ passing through the origin.

Definition 4.6. 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 $ac \sim bd$.

Example 4.7. Let $n \in \mathbb{Z}$, $n \geq 1$. The relation $a \sim b \Leftrightarrow n|(b-a)$ is an equivalence relation in $\mathbb{Z}$. Indeed, reflexivity and symmetry are obvious. For transitivity, observe that if $n|(b-a)$ and $n|(c-b)$, then $n|((b-a)+(c-b)) \Rightarrow n|(c-a)$. It is also a congruence relation in the commutative ring $\mathbb{Z}$. We have:

$$a \sim b, \;\; c \sim d \;\; \Rightarrow n|(b-a), \;\; n|(d-c) \;\; \Rightarrow n|(b+d-a-c) \;\; \Rightarrow (a+c) \sim (b+d).$$

$$a \sim b, \;\; c \sim d \;\; \Rightarrow n|(b-a), \;\; n|(d-c) \;\; \Rightarrow n|c(b-a)+b(d-c) = bd-ac \;\; \Rightarrow ac \sim bd.$$

Proposition 4.8. *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].

Proof: The addition $\bar{a} + \bar{b} = \overline{a+b}$ and multiplication $\bar{a}\bar{b} = \overline{ab}$ are well defined, which follows from the definition of the congruence. The congruence classes $\bar{0}$ and $\bar{1}$ are the additive and multiplicative identity elements. The axioms are easy to check.

Proposition 4.9. *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.

Proof: (1) The fact that I is an abelian group with respect to addition is equivalent to $\sim$ being an equivalence relation.
(2) Suppose that $I \subset A$ is an ideal, and set $a \sim b \Leftrightarrow (a-b) \in I$. We check the axioms of a congruence. $a \sim b$ and $c \sim d$ implies $(a+c) \sim (b+d)$ since $(b-a)+(d-c) = b+d-a-c \in I$. The multiplicative property of the ideal implies $ac \sim bd$: $bd - ac = b(d-c) + c(b-a) \in I$.
(3) Let $\sim$ is a congruence relation in A, then set $I = \{a \in A, \; a \sim 0\}$. Then if $x \in I$ and $a \in A$, we have $x \sim 0$ and $a \sim a$ which implies $xa = ax \sim 0$, and therefore $xa = ax \in I$.

[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*.

Definition 4.10. 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.

Example 4.11. In the example 4.7, if $n \geq 2$, we obtain the quotient ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n.

Exercise 4.12. Consider the polynomial ring $\mathbb{R}[x]$ and the ideal $J = ((x^2 - 1))$ (see Example 3.19). The set $\mathbb{R}[x]/J$ is a commutative ring. Note that it is not an integral domain: $\overline{(x-1)} \cdot \overline{(x+1)} = \overline{0}$ in $\mathbb{R}[x]/J$.

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.*

Proof: If $I = \{0\}$, then $I = (0)$ is a principal ideal. Now suppose that $I \neq \{0\}$. If $a \in I$, then $-a \in I$, and so $|a| \in I$, so that I contains positive integers. Let $d \in I$ be the smallest positive integer that belongs to I (note that we use the well-ordering principle here). Now let $n \in I$ for some $n \in \mathbb{Z}$. By the Euclidean division, we have $n = kd + r$, where $k \in \mathbb{Z}$ and $0 \leq r \leq d - 1$. Then, since I is an ideal, we have $kd \in I$ and $n - kd = r \in I$. Since d was chosen to be the smallest positive integer in I, this implies that $r = 0$ and $n = kd$. This shows that $I = (d) \subset \mathbb{Z}$ is a principal ideal.

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 $d = \gcd(a_1, a_2, \dots a_n)$.*

Proof: By definition the elements of I are of the form $a_1x_1 + a_2x_2 + \dots a_nx_n$, where $x_i \in \mathbb{Z}$. We proceed by induction on n. If $n = 1$, $d = a_1$. If $n = 2$, then the equation $a_1x_1 + a_2x_2 = c$ has a solution for integers x_1, x_2 if and only if $c \in \gcd(a_1, a_2)$ (Bezout's theorem). Then suppose the statement holds for n. Let $d_n = \gcd(a_1, a_2, \dots a_n)$. The equation

$$a_1x_1 + a_2x_2 + \dots a_nx_n + a_{n+1}x_{n+1} = d_ny + a_{n+1}x_{n+1} = c$$

has a solution if and only if c is a multiple of $\gcd(d_n, a_{n+1}) = d_{n+1}$. The conclusion follows.

Example 5.4. Let I be the smallest ideal in $\mathbb{Z}$ containing the numbers $\{36, 192, 60\}$. Then $I = (d) \subset \mathbb{Z}$, where $d = \gcd(2^2 \cdot 3^2, 2^6 \cdot 3, 2^2 \cdot 3 \cdot 5) = 12$.

Recall that for a natural number d, the ideal $(d) \in \mathbb{Z}$ defines a congruence relation $a \sim b \Leftrightarrow (a - b) \in (d)$, and that for $d \geq 2$, the quotient set $\mathbb{Z}/d\mathbb{Z}$ has a structure of a commutative ring (Examples 4.7, 4.11). Let us consider the multiplicative and additive structure of the obtained ring $\mathbb{Z}/d\mathbb{Z}$.

Example 5.5. Let $d = 6$. To simplify the notation we will write n for the congruence class $[n]_6$ in the tables below. Then the ring $\mathbb{Z}/6\mathbb{Z}$ has the following addition and multiplication tables:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

In particular, we notice that $[2]_6, [3]_6$ and $[4]_6$ are the nontrivial zero divisors, and $[1]_6, [5]_6$ are invertible elements in $\mathbb{Z}/6\mathbb{Z}$. The number of the invertible elements equals to $\phi(6) = 2$, which agrees with Corollary 2.10. In particular, $\mathbb{Z}/6\mathbb{Z}$ is not a field.

Recall from Corollary 2.19 that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n = p$ is a prime.

Example 5.6. Consider the ring $\mathbb{Z}/5\mathbb{Z}$. The multiplication table is the following (here again we write n for the class $[n]_5$ for simplicity):

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

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 $\mathrm{im}(f) \subset B$ is a subring in B (a subring is an additive subgroup of a ring containing 1 and closed with respect to the multiplication).*

Proof: (1) If $f(a) = 0$ and $f(b) = 0$, then $f(a \pm b) = 0$, therefore $\ker(f)$ is a subgroup with respect to addition. If $c \in A$ and $a \in \ker(f)$, we have $f(ac) = f(a)f(c) = 0$, and therefore the ideal property is satisfied.
(2) If $f(a), f(b) \in \mathrm{im}(f)$, then We have $f(a) \pm f(b) = f(a \pm b) \in \mathrm{im}(f), f(a)f(b) = f(ab) \in \mathrm{im}(f)$, and $f(a+0) = f(a) + f(0) = f(a)$, $f(1_A) = 1_B$, therefore $\mathrm{im}(f) \subset B$ is a subring.

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

Proof: The only subring of $\mathbb{Z}/m\mathbb{Z}$ is $\mathbb{Z}/m\mathbb{Z}$ itself. Indeed, a subring is an additive subgroup that contains $[1]_m \in \mathbb{Z}/m\mathbb{Z}$, and $[1]_m$ generates the whole $\mathbb{Z}/m\mathbb{Z}$ by addition. Then, $f([0]_n) = f(n[1]_n) = nf([1]_n) = n[1]_m = [0]_m$, which implies that $m|n$. (Alternatively, you can argue that $\ker(f)$ must be an ideal in $\mathbb{Z}/n\mathbb{Z}$, and the only ideals in $\mathbb{Z}/n\mathbb{Z}$ are generated by the classes $[k]_n$ such that $k|n$). Finally, $f([a]_n) = f(a[1]_n) = af([1]_n) = a[1]_m = [a]_m$.

Example 6.4. There exists a unique ring homomorhism $f_1 : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, such that $\mathrm{im}(f_1) = \mathbb{Z}/3\mathbb{Z}$, and $\ker(f_1) = \{[0]_6, [3]_6\}$, which is an ideal in $\mathbb{Z}/6\mathbb{Z}$. There exists a unique ring homomorphism $f_2 : \mathbb{Z} \to \mathbb{Z}/18\mathbb{Z}$ that sends $a \in \mathbb{Z}$ to $[a]_{18} \in \mathbb{Z}/18\mathbb{Z}$. The kernel of f_2 is the ideal $(18) \subset \mathbb{Z}$, and the image is the whole ring $\mathbb{Z}/18\mathbb{Z}$. There is no ring homomorphisms $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$, because 12 does not divide 6.

Proposition 6.5. *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 $d \in \mathbb{Z}$.*

Proof: Since $\tau(1) = 1_A$, we have $\tau(k) = \tau(1+1+\ldots+1) = k \cdot 1_A$ for any $k \in \mathbb{Z}$. This shows that the homomorphism is unique. We have $\ker(\tau) = \{0\}$ if $k \cdot 1_A \neq 0_A$ for any $k \in \mathbb{Z}$. Otherwise if there exists a minimal $d \in \mathbb{Z}^+$ such that $d \cdot 1_A = 0_A$, we have $\ker(\tau) = (d) \subset \mathbb{Z}$.

Definition 6.6. 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:

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

Example 6.7. The characteristic of the ring $\mathbb{Z}/m\mathbb{Z}$ is m for any $m \geq 2$. The ring of rational numbers $\mathbb{Q}$ is of characteristic 0.

Proposition 6.8. *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.*

Proof: We have $\tau(n) = 0$ in A, and $n = mk$ with nontrivial divisors m, k. Let $a = \tau(m)$ and $b = \tau(k)$. Then $a \neq 0$ and $b \neq 0$ in A, because otherwise $c_A < n$. We have $ab = \tau(m)\tau(k) = \tau(mk) = \tau(n) = 0$, therefore $a, b \in A$ are nontrivial zero divisors.

Corollary 6.9. *The characteristic of a field is either 0, or a prime number p.*

Definition 6.10. 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 $0_{A\times B} = (0_A, 0_B)$.

Example 6.11. Let $n, m \in Z$, $n, m \geq 2$ Then the characteristic of the ring $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is $\mathrm{lcm}(n, m)$. Indeed, $\tau(1) = ([1]_n, [1]_m)$, and we have $a([1]_n, [1]_m) = ([0]_n, [0]_m)$ if and only if $n|a$ and $m|a$. Then a is minimal with this property if $a = \mathrm{lcm}(n, m)$. More generally, if A and B are two commutative rings, and $c_A \neq 0$, $c_B \neq 0$, then $c_{A\times B} = \mathrm{lcm}(c_A, c_B)$. The same proof holds.

Corollary 6.12. *The converse to Corollary 6.9 is false: there exists a ring with characteristic p that is not a field.*

Proof: the characteristic of the ring $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is $\mathrm{lcm}(p, p) = p$. However, the ring $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ has nontrivial zero divisors: for example $([1]_p, [0]_p) \cdot ([0]_p, [1]_p) = ([0]_p, [0]_p)$.

Example 6.13. The characteristic of the ring $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is 0: there is no $a \in \mathbb{Z}^+$ such that $a(1, [1]_n) = (0, [0]_n)$. The characteristic of the polynomial ring $\mathbb{Z}/n\mathbb{Z}[x]$ is n: we have $\tau(1) = 1 \in \mathbb{Z}/n\mathbb{Z}[x]$, and $\ker(\tau) = (n) \subset \mathbb{Z}$.

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 4.10).

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 $f : \bar{x}_{I\cap J} \to (\bar{x}_I, \bar{x}_J)$.

Proof. Clearly f is a ring homomorphism (check that it is well defined and respects the ring operations). We will show that for any two elements $a_1, a_2 \in A$, there is an element $a \in A$ such that $a \equiv a_1 \pmod I$ and $a \equiv a_2 \pmod J$. Moreover, if there are two such elements a and b, then $a \equiv b \pmod{I\cap J}$. This will imply that the map $f : A/(I\cap J) \to A/I \times A/J$ given by the diagonal map $f : x \to (x, x)$ is an isomorphism of rings.
Indeed, $a_1 - a_2 \in A = I + J$, and therefore there exist $i \in I$ and $j \in J$ such that $a_1 - a_2 = j - i$. Then set $a = a_1 + i = a_2 + j$, and we have $a \equiv a_1 \pmod I$ and $a \equiv a_2 \pmod J$. Therefore the map f is surjective.
If $b \equiv a_1 \pmod I$ and $b \equiv a_2 \pmod J$, then $b = a_1 + i' = a_2 + j'$, and $a - b = i - i' = j - j' \in J \cap I$. Therefore the map f is injective.
By construction f is a ring homomorphism, therefore it is a ring isomorphism.

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 $a + mn\mathbb{Z}$.*

Proof: By Bezout's theorem there exist $x, y \in \mathbb{Z}$ such that $xm + yn = 1$. We have that the ideal $(m) + (n)$ contains 1 and therefore it is equal to $\mathbb{Z}$. Then we can apply theorem 7.1. In this case it assures that there exist an integer $a \in \mathbb{Z}$ such that $[a]_n = [a_1]_n$ and $[a]_m = [a_2]_m$, and moreover, all such numbers $a \in \mathbb{Z}$ differ by an element in the ideal $(n) \cap (m) = (nm)$, the last equality follows since $\gcd(n, m) = 1$.

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

Proof: The constructed map respects the ring operations. To show that it is a well defined bijection, we proceed by induction on n. If $n = 1$, there is nothing to prove, if $n = 2$, this is a direct consequence of Theorem 7.1: since $\gcd(d_1, d_2) = 1$, the ideals (d_1) and (d_2) in $\mathbb{Z}$ satisfy $(d_1) + (d_2) = \mathbb{Z}$, and the ideal $(d_1) \cap (d_2) = (d_1 d_2)$. Now suppose the Theorem holds for n. This means that there exists an integer $a \in \mathbb{Z}$ such that for any set of integers $a_1, \dots a_n \in \mathbb{Z}$, we have $a - a_1 \in (d_1)$, $a - a_2 \in (d_2)$, and so on until $a - a_n \in (d_n)$, and if there is another such integer $b \in \mathbb{Z}$, then $a - b \in (d) = (d_1 d_2 \dots d_n)$. Now suppose that d_{n+1} is such that $\gcd(d_i, d_{n+1}) = 1$ for any $1 \leq i \leq n$. Then $\gcd(d, d_{n+1}) = 1$, and we can apply the case $n = 2$ again to find $c \in \mathbb{Z}$ such that for any $a_{n+1} \in \mathbb{Z}$, we have $c - a \in (d)$ and $c - a_{n+1} \in (d_{n+1})$. Moreover, if s is another such element, then $c - s \in (d) \cap (d_{n+1}) = (d_1 d_2 \dots d_n d_{n+1})$. Therefore, the constructed map is bijective.

Example 7.4. There is an isomorphism of rings: $\mathbb{Z}/60\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Corollary 7.5. *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 $a + d\mathbb{Z}$.

Proof: since the numbers $\{d_1, \dots d_r\}$ are pairwise coprime, we have $(d_i) + (d_j) = \mathbb{Z}$ for any two ideals among $(d_1), \dots (d_r)$. Then Theorem 10.1 provides a ring isomorphism

$$Z/(d_1 d_2 \cdots d_r) \simeq \mathbb{Z}/(d_1) \times \mathbb{Z}/(d_2) \times \dots \times \mathbb{Z}/(d_r),$$

that ensures the existence of $a \in Z$ such that $a - a_i \in (d_i)$. Moreover, if b is another such element, then $a - b \in (d_1) \cap (d_2) \cap \dots \cap (d_r) = (d_1 d_2 \cdots d_r) \subset \mathbb{Z}$.

Remark 7.6. The proof of Theorem 10.1 provides a method to solve systems of congruences: suppose you have to solve a system of congruences modulo $d_1, d_2, \dots d_r$ where the elements $d_1, d_2, \dots d_r$ 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_1d_2. The product d_1d_2 is coprime to d_3. Solve these two congruences, obtaining a congruence modulo $d_1d_2d_3$. The product $d_1d_2d_3$ 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 $d = d_1d_2 \dots d_k$ 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 $D_ix_i + d_iy_i = 1$. Then $x = \sum_{i=1}^{k} a_iD_ix_i$. Indeed, $x \equiv a_iD_ix_i \pmod{d_i}$, because $d_i | D_j$ for $j \neq i$. Therefore, $x \equiv a_i(1 - d_iy_i) \pmod{d_i} \equiv a_i \mod (d_i)$. The solution is determined modulo D.

Exercise 7.7. (Exam 2017). Explain, citing a result from the course and checking that the hypothesis is satisfied, why the following system of congruences has a solution:

$$\begin{cases} a \equiv 11 \pmod{13} \\ a \equiv -1 \pmod{5} \\ a \equiv 3 \pmod{4} \\ a \equiv 7 \pmod{3} \end{cases}$$

Find a solution $a \in \mathbb{Z}$ of this system. Describe the set of all solutions of this system.

Solution. A solution exists because the numbers $\{3, 4, 5, 13\}$ are pairwise coprime. Start solving congruences consecutively starting from the simplest, for example $a \equiv 1 \pmod 3$ and $a \equiv -1 \pmod 4$: $3t + 1 = 4s - 1$, $t = 6, s = 5$. Then we have $a \equiv 19 \pmod{12}$. Consider it together with $a \equiv -1 \pmod 5$: here we see that 19 works and we have $a \equiv 19 \pmod{60}$. Adding the last congruence, $a \equiv -2 \pmod{13}$, we compute $60x + 19 = 13y - 2$, then $60x - 13y = -21$, and we have for example $x = -1$, $y = -3$, and $a = 60(-1) + 19 = -41$. Finally $a \equiv -41 \pmod{780}$. The set of all solutions is $\{-41 + 780n, n \in \mathbb{Z}\}$. The smallest positive solution is $a = 739$.

Remark 7.8. 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 7.9. *Let $n, m \in \mathbb{Z}$ be such that $\gcd(n, m) = 1$. Then we have for the Euler's totient function:*

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

Proof: Since by Corollary 7.5 the rings $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ are isomorphic, their groups of units are also isomorphic, in particular the order $|(\mathbb{Z}/mn\mathbb{Z})^*| = \varphi(mn)$ equals to the order $|(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})|^* = |(\mathbb{Z}/nZ)|^* \times |(\mathbb{Z}/m\mathbb{Z})|^* = \varphi(n)\varphi(m)$.

Example 7.10. Recall from the beginning of the course that $\phi(p) = p - 1$ and $\phi(p^n) = p^n - p^{n-1}$ for any prime $p \in \mathbb{Z}$. Compute $\phi(64680)$.
We have $64680 = 2^3 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11$, and therefore $\phi(64680) = (8 - 4) \cdot 2 \cdot 4 \cdot (49 - 7) \cdot 10 = 320 \cdot 42 = 13440$.

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 $A[x] = \{a_0 + a_1x + \ldots + a_nx^n\}$, where $n \in \mathbb{N}$ and $a_0, a_1, \dots a_n$ 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 $f(x) = a_0 + a_1x + \ldots$ 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 $\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x))$.

Proof: Consider

$$f(x)g(x) = (a_0 + a_1x + \ldots + a_nx^n)(b_0 + b_1x + \ldots b_mx^m) = a_0b_0 + \ldots + a_nb_mx^{n+m}.$$

If A is an integral domain, $a_n \neq 0$ and $b_m \neq 0$ imply $a_nb_m \neq 0$, and $\deg(f(x) \cdot g(x)) = \deg(f(x) + \deg(g(x))$. If $f(x) = 0$, then $f(x)g(x) = 0 \cdot g(x) = 0$, and $\deg(f(x)g(x)) = -\infty + \deg(g(x)) = -\infty$.

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.*

Proof: If $f(x)g(x) = 0$, then $\deg(f(x)g(x)) = -\infty = \deg(f(x)) + \deg(g(x))$, since A is an integral domain. This implies $\deg(f(x)) = -\infty$ or $\deg(g(x)) = -\infty$, or both, and so at least one of $f(x) = 0$ or $g(x) = 0$. A similar degree argument shows that the invertible elements in $A[x]$ are the invertible constants.

Example 8.5. The ring $\mathbb{Z}[x]$ is an integral domain. The ring $\mathbb{Z}/6\mathbb{Z}[x]$ is not an integral domain: $2x \cdot 3x = 0 \in \mathbb{Z}/6\mathbb{Z}[x]$.

Theorem 8.6. *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 $\deg(r(x)) < \deg(d(x))$.*

Proof: If $\deg(f(x)) < \deg(d(x))$, then take $q(x) = 0$, $r(x) = f(x)$.
If $\deg(f(x)) \geq \deg(d(x))$, then if $f(x) = a_0 + \ldots + a_m x^m$, $d(x) = b_0 + \ldots b_n x^n$, consider

$$f(x) - d(x) \cdot \frac{a_m}{b_n} x^{m-n} = p(x),$$

with $\deg(p(x)) < \deg(f(x))$. Repeat with $p(x)$ until $f(x) - d(x) \cdot \left(\frac{a_m}{b_n} x^{m-n} + \ldots\right) = r(x)$ with $\deg(r(x)) < \deg(d(x))$ (it can happen that $r(x) = 0$). The process terminates because the degree is strictly decreasing.

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 $\nu(r) < \nu(b)$.

Example 9.2. The ring $\mathbb{Z}$ is a Euclidean domain with $\nu(k) = |k|$ for any integer k. Any field F is a Euclidean domain. Indeed, we have $a = qb + 0$ for any $b \neq 0$ in F. In particular, we can define the function $\nu : F \setminus \{0\} \to \mathbb{N}$ by $F(b) = 0$ for any $b \in F$.

Exercise 9.3. Check that the ring $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \ : \ a, b \in \mathbb{Z}\}$ of Gaussian integers is a Euclidean domain with $\nu(a + ib) = a^2 + b^2$.

Corollary 9.4. *If F is a field, then the ring of polynomials $F[x]$ is a Euclidean domain.*

Proof: By Theorem 8.4, $F[x]$ is an integral domain. By Theorem 8.6, the function $\deg : F[x] \setminus \{0\} \to \mathbb{N}$ satisfies the conditions of the definition of a Euclidean domain.

Theorem 9.5. *A Euclidean domain is a principal ideal domain.*

Proof: Let E be a Euclidean domain, and $I \subset E$ an ideal. If $I = \{0\}$, the ideal I is principal. Suppose $I \neq \{0\}$, and let $d \in I$ with $d \neq 0$ and such that $\nu(d)$ is minimum on I. Suppose $a \in I$. Since E is a Euclidean domain, there exist elements $q, r \in E$ such that $a = qd + r$, and either $r = 0$, or $\nu(r) < \nu(d)$. Since $a, d \in I$, we have $r \in I$, and therefore by the choice of d, $\nu(r) \geq \nu(d)$. This implies $r = 0$, and $I = (d) \subset E$ is a principal ideal. Therefore, any ideal in E is principal.

Remark 9.6. Note that the proof of Theorem 9.5 generalizes the proof of the same property for integers. The notion of Euclidean domain generalizes the Euclidean division property in $\mathbb{Z}$.

Corollary 9.7. *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.*

Proof: Theorem 9.5.

Definition 9.8. 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 9.9. 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 $v \in A^*$).

Exercise 9.10. Find the associates of each element in the ring $\mathbb{Z}$.

Definition 9.11. 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 $d = \text{gdc}(a, b)$. 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 $l = \text{lcm}(a, b)$.

Note that $d = \gcd(a, b)$ and $l = \text{lcm}(a, b)$ is not necessarily unique for a couple of elements $a, b \in A$.

Proposition 9.12. *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.*

Proof: We have $d_1 = xd_2$ and $d_2 = yd_1$. Derive that $d_2 = xyd_2$. Then $d_2(1 - xy) = 0$, and since A is an integral domain, if $d_2 \neq 0$, we have $xy = 1$ (if $d_2 = 0$, then $d_1 = 0$ and they are associates). The proof for the least common multiples is the same.

Proposition 9.13. *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 $\text{lcm}(a, b) = ab$.

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

Proof.

(a) If $d|a, d|b$, then $d|r = a - qb$. If $d|b$ and $d|r$, then $d|a$. So the same argument as we used for integers shows that $r_n = \gcd(a, b)$.

(b) Let $d \in E$ be an element generating the ideal (a, b). Then $a, b \in (d)$ and therefore $d|a$ and $d|b$. SInce $d \in (a, b)$, we have $d = xa + yb$ and if $c|a, c|b$ then $c|d$, so $d = \gcd(a, b)$.

(c) If $xa + yb = 1$, then $xca + ycb = c$ and $a|xca$ and $a|cb$, therefore $a|c$.

(d) similarly, if $xa + yb = 1$, then $xca + ycb = c$, and we have $ab|ca$ and $ab|cb$ since $a|c$ and $b|c$, and therefore $ab|c$.

(e) Let $m \in E$ be an element generating the ideal $(a) \cap (b)$. Then $a|m$ and $b|m$. If $a|t$ and $b|t$ for some element $t \in E$, then $t \in (a)$ and $t \in (b)$, and therefore $t \in (m)$ and $m|t$. Therefore $m = \text{lcm}(a, b)$.

Exercise 9.14. Let I be the smallest ideal in $\mathbb{R}[x]$ that contains the polynomials $(x^2 - 1)$, $(x^2 - 6x + 5)$. Find a polynomial $p(x)$ that generates this ideal.

Remark 9.15. 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 9.12 $d_1(x) = ud_2(x)$, 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: $(d_1) = (d_2) = (d)$.

Example 9.16. Find a $\gcd(f(x), g(x))$ in $\mathbb{R}[x]$, where $f(x) = x^3 + 6x^2 - 3x - 4$ and $g(x) = x^2 - 5x + 4$. We use Euclid's algorithm: $f(x) = (x + 11)g(x) + 48x - 48$, therefore $r_1(x) = 48x - 48$. Then $g(x) = r_1(x)(\frac{1}{48}x - \frac{1}{12})$. Therefore $\gcd(f(x), g(x)) = 48x - 48$. By the previous remark, we can find the unique monic polynomial $d(x) = \gcd(f(x), g(x)) = x - 1$.

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 $(a) \cap (b) = (\text{lcm}(a, b)) \subset E$ and $(a) + (b) = (\gcd(a, b)) \subset E$.
3. $\gcd(a, b)$ and $\text{lcm}(a, b)$ 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 $m_1, m_2, \dots m_r$ elements such that $\gcd(m_i, m_j) = 1$ for any two indices $1 \le i \ne j \le r$. Let $m = m_1 m_2 \dots m_r$. Then the map*

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

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

Proof: The homomorphism property is clear from the construction. Suppose $a_1, a_2 \dots a_r$ are arbitrary elements of A. Then we will show that there exists $a \in A$ such that $a \equiv a_i \pmod{m_i}$ for all $i = 1, \dots r$, which will show the surjectivity of the map f.
We will use properties of Euclidean domains (Proposition 9.13). First note that if $\gcd(m_i, m_j) = 1$, for any pair $i \ne j$, then $\gcd(m_i, m_1 \cdots m_{i-1} m_{i+1} \cdots m_r) = 1$ (Property (c) in Proposition 9.13). Then there exist $x, y \in A$ such that $x m_i + y m_1 \cdots m_{i-1} m_{i+1} \cdots m_r = 1$, and therefore $(m_1) + (m_1) \cap \dots (m_{i-1}) \cap (m_{i+1}) \cap \dots \cap (m_r) = A$. In particular, $(m_1) + (m_2) = A$ and by Theorem 7.1 we have $a_{12} \in A$ such that $a_{12} \equiv a_1 \pmod{m_1}$ and $a_{12} \equiv a_2 \pmod{m_2}$. Now $(m_3) + (m_1) \cap (m_2) = A$ and so by Theorem 7.1 there exists $a_{123} \in A$ such that $a_{123} \equiv a_3 \pmod{m_3}$ and $a_{123} \equiv a_{12} \pmod{m_1 m_2}$, so that $a_{123} \equiv a_1 \pmod{m_1}$ and $a_{123} \equiv a_2 \pmod{m_2}$. In particular, the ideal $(m_1) \cap (m_2) = (\mathrm{lcm}(m_1, m_2)) = (m_1 m_2)$ by Proposition 9.13 (e). Then proceed by induction.
For injectivity of f, if there are two elements a, b such that $\bar{a}_{(m_i)} = \bar{b}_{(m_i)}$ for all i, then $a - b$ lies in the intersection of the ideals $(m_1) \cap (m_2) \cap \dots \cap (m_r)$, that is equal to (m).

Now we can apply this theorem to polynomial rings. Recall that if F is a field, the ring $F[x]$ of polynomials with coefficients in F is a Euclidean domain.

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

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

Exercise 10.3. Let $F_3 = \mathbb{Z}/3\mathbb{Z}$ denote the field of 3 elements. Find the set of all solutions $f(x) \in F_3[x]$ of the system of congruences

$$\begin{cases} f(x) \equiv x \pmod{(x^2+1)} \\ f(x) \equiv 1 \pmod{x} \\ f(x) \equiv x+2 \pmod{(x^2-1)} \end{cases}$$

Solution. First we need to check that the polynomials $\{f_1(x) = x^2+1,\ f_2(x) = x,\ f_3(x) = x^2-1\}$ are pairwise coprime in $F_3[x]$. For example, $\gcd(f_1(x), f_2(x)) = 1$ if we can find $g_1(x), g_2(x) \in F_3[x]$ such that $f_1(x)g_1(x) + f_2(x)g_2(x) = 1$. We have: $(x^2+1) \cdot 1 + x \cdot (-x) = 1$. Similarly, we have $x \cdot x + (x^2-1)(-1) = 1$ and $(x^2+1)(-1) + (x^2-1) \cdot 1 = 1 \in F_3$. So we can apply the Chinese remainder theorem.
From the first two congruences we get $f(x) \equiv x^2 + x + 1 \pmod{(x(x^2+1))}$ (an obvious solution). Then we need to solve it together with the congruence $f(x) \equiv x+2 \pmod{(x^2-1)}$. We notice that $x^2 + x + 1 = (x^2-1) + x + 2$, so we have that $f(x) = x^2 + x + 1$ is one solution. To obtain the complete set of solutions, by the Chinese remainder theorem we need to add any element in the ideal $(x(x^2+1)(x^2-1)) = (x^5 - x) \subset F_3[x]$. The complete set of solutions is $\{x^2 + x + 1 + g(x)(x^5 - x)\}_{g(x) \in F_3[x]}$.

11 Irreducible elements in Euclidean domains.

We consider Euclidean domains, that are also principal ideal domains (Theorem 9.5), where all ideals are generated by a single element. Let $I \subset A$ be an ideal. Recall that an ideal $I \subset A$ in a commutative ring A defines a quotient ring A/I (see Definition 4.10). The quotient ring A/I is the commutative ring of equivalence classes with respect to the equivalence relation $a \sim b$ if and only if $a - b \in I$.

When is A/I a field?

Definition 11.1. Let A be a commutative ring. The element $c \in A$ is irreducible if c is not a unit in A (c is not invertible in A), $c \ne 0$, 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.

Example 11.3. Consider the ring $\mathbb{Z}/6\mathbb{Z}$. We have $[2]_6 = [2]_6 \cdot [4]_6$, so $[2]_6$ is not irreducible. Also, $[3]_6 = [3]_6 \cdot [3]_6$, and $[4]_6 = [4]_6 \cdot [4]_6$, so they are not irreducible. The elements $[1]_6$ and $[5]_6$ are units: $[5]_6 \cdot [5]_6 = [1]_6$. Therefore there are no irreducible elements in $\mathbb{Z}/6\mathbb{Z}$. Note that $\mathbb{Z}/6\mathbb{Z}$ is a principal ideal ring, but not a principal ideal domain: it has zero divisors. In a PID, any maximal ideal is generated by an irreducible element (see the following Proposition). Here we have two maximal ideals: $([2]_6) \subset \mathbb{Z}/6\mathbb{Z}$ and $([3]_6) \subset \mathbb{Z}/6\mathbb{Z}$ but they are not generated by irreducible elements.

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 11.4. *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.*

Proof: Let $p \in A$ be irreducible. Suppose there is an ideal $I \subset A$ such that $(p) \subsetneq I \subsetneq A$. Then $I = (d)$ for a $d \in A$, and $p = dt$ for an element $t \in A$. Since p is irreducible, this implies that either d or t is a unit. If d is a unit, then $(d) = A$. If t is a unit, then $d = t^{-1}p$, d and p are associates. Then $(d) \subset (p)$ and $(p) \subset (d)$, which implies $(d) = (p)$. We have a contradiction in both cases, therefore no such ideal I exists.
Conversely, let (p) be maximal in A. If there exist non-units $y, z \in A$ such that $p = yz$, then $(p) \subset (y) \subsetneq A$, where $y \neq A$ since y is not a unit. If we suppose that $(y) = (p)$, then $y = tp$ where t is a unit, which implies $p = yz = ptz$ and $p(1 - tz) = 0$. Since $p \neq 0$, we have that z is a unit, contradiction. Therefore, $(p) \subsetneq (y)$ and (p) is not maximal, contradiction.

Proposition 11.5. *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.

Proof:

(a) For (a), let $\gcd(a, b) = d$. Then by Bezout's theorem, there exist $x, y \in A$ such that $xa + yb = 1$ if and only if $d = 1$, and this holds if and only if $\bar{y}\bar{b} = \bar{1}$ in the quotient ring A/I, which means that $\bar{b}$ is a unit.

(b) If $\gcd(a, b) = d \neq 1$, then there exist $s, t \in A$ such that $a = dt$ and $b = ds$. Then $bt = dts = as$, and so $\bar{b}\bar{t} = \bar{0}$, but $\bar{t} \neq \bar{0}$ and $\bar{b} \neq \bar{0}$, so $\bar{b}$ is a nontrivial zero divisor in A/I. Conversely, if $\bar{b}\bar{t} = \bar{0}$, then there are no x, y such that $ax + by = 1$ by (a) and $\gcd(a, b) \neq 1$.

(c) follows from (a): every nonzero element in A/I is a unit if and only if $\gcd(a, k) = 1$ for $k \in A$ unless k is a multiple of a. This means that a is irreducible.

Corollary 11.6. *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 11.6).

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 $\text{lcm}(f(x), g(x))$, unique up to multiplication by units. They generate the ideals $(f(x))+(g(x)) = (\gcd(f(x), g(x)))$ and $(f(x)) \cap (g(x)) = (\text{lcm}(f(x), g(x)))$.

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.*

Proof: We use that $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$. (Proposition 8.3). Then if $\deg(f(x)) = 1$, we can only have $f(x) = h(x)g(x)$ if one of the polynomials $h(x)$ or $g(x)$ is a nonzero constant, that is a unit in F. If $\deg(f(x)) = 2$ or 3, then $f(x) = h(x)g(x)$ with $h(x), g(x)$ two non-units implies at least one of them is of degree 1. Then we have, say $h(x) = ax - b$ for element $a, b \in A$ with $a \neq 0$, and $x = b/a$ is a root of $f(x)$.

Example 12.3. Let $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ and consider the ring $\mathbb{F}_5[x]$. The polynomials $f_1(x) = x - 3$ and $f_2(x) = 3x^2 + 2x + 1$ are irreducible in $\mathbb{F}_5[x]$ (it is enough to try for roots $x = \pm 1, \pm 2$), but $f_3(x) = 2x^3 - 3x^2 + x + 1$ is not: $f_3(-1) = -2 - 3 - 1 + 1 = [0]_5$. Using polynomial division we get $f_3(x) = (x + 1)(2x^2 + 1)$.

Proposition 12.4. *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.*

Proof: See PS12.

Example 12.5. Show that the polynomials $f_1(x) = x^3 + 3x^2 - 7x + 2$ and $f_2(x) = 2x^3 + 4x^2 + 11x + 1$ are irreducible in $\mathbb{Q}[x]$. The first polynomial is monic, and such that any rational root is of the form $\pm r$, where $r|2$, therefore we only need to check $f_1(\pm 1) \neq 0$, $f_1(\pm 2) \neq 0$, which is true. For $f_2(x)$, any rational root is of the form $\frac{r}{s}$, where $s|2$ and $r|1$. Therefore it is sufficient to check $f_2(\pm 1) \neq 0$ and $f_2(\pm \frac{1}{2}) \neq 0$, which is true. Since the degrees of both polynomials are 3, having no roots means they are irreducible.

Proposition 12.6. *(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 $\mathbb{Z}[x]$).*

Proof: Let $h(x) = h_0 + h_1 x + \ldots + h_k x^k, g(x) = g_0 + g_1 x + \ldots g_m x^m \in F(x)$ such that $g(x)h(x) = f(x)$. Then $h_0 g_0 = a_0$, and $h_k g_m = a_{m+k} = a_n$. We have that $p|a_0 = g_0 h_0$, but $p^2 \nmid g_0 h_0$, so for example $p|g_0$ and $p \nmid h_0$. We know that p cannot divide all g_i, because then p would divide all a_i. Let t be the smallest index such that $p \mid g_0, p \mid g_1, \ldots p \mid g_{t-1}$, but $p \nmid g_t$. Then $t \leq \deg(g(x)) < \deg(f(x)) = n$. Also we have $a_t = \sum_{j=0}^{t} g_j h_{t-j} = g_t h_0 + \sum_{j=0}^{t-1} g_j h_{t-j}$. The second summand is divisible by p, but $p \nmid g_1 h_0$, and therefore $p \nmid a_t$, contradiction.

Example 12.7. (a) Show that polynomial $2x^6 + 9x^4 - 15x^2 - 6x + 3$ is irreducible over $\mathbb{Q}[x]$.
(b) Let p be a prime. Then $g(x) = x^k - p$ is irreducible for any $k \geq 1$.
Both properties follow directly from the Eisenstein's criterion: (a) with $p = 3$ and (b) with $p = p$.

Proposition 12.8. *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 $x^i + (f(x))$.

Proof: By the Euclidean division for any polynomial $p(x) \in F[x]$ we can write $p(x) = f(x)q(x) + r(x)$ for some $q(x), r(x) \in F[x]$ with $\deg(r) < \deg(f)$. So any congruence class modulo $(f(x))$ can be written in the required form. Moreover, the congruence classes $\{\overline{x^i}\}_{i=0}^{n-1}$ are linearly independent over F. Indeed, if $\sum_i b_i \overline{x^i} = \overline{0} \in F[x]/(f(x))$, then the polynomial $\sum_i b_i x^i \in F[x]$ lies in the ideal generated by $f(x)$, and therefore it is divisible by $f(x)$ of degree n, which is impossible.

Corollary 12.9. *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.*

Proof: By Proposition 12.8 any element of $F[x]/(f(x))$ can be written uniquely as a polynomial with coefficients in F of a degree strictly smaller than n.

Exercise 12.10. Consider the field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ and show that the polynomial $f(x) = x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. Consider the field $\mathbb{F}_2[x]/(f(x))$ and list all its elements. Find the inverse to the element $\bar{x}$ in $\mathbb{F}_2[x]/(f(x))$.

Solution: $f(0) \neq 0$, $f(1) \neq 0$, therefore a polynomial of degree 3 is irreducible over $\mathbb{F}_2[x]$. There are $2^3 = 8$ total elements in the field $\mathbb{F}[x]/(f(x))$, and proposition 12.8 gives a method to list them:

$$\{\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1}\}.$$

To find the inverse to $\overline{x}$, we should solve an equation $x \cdot g(x) + (x^3 + x + 1)h(x) = 1$. We have $\overline{g(x)} = \overline{x^2+1}$.

Exercise 12.11. (Exam 2017).

(a) Show that the polynomial $x^2 + x + 1$ is the only irreducible polynomial of degree 2 over $\mathbb{F}_2$.

(b) Show that $x^4 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.

(c) Let $K = \mathbb{F}_2[x]/(x^4 + x + 1)$. Show that K is a field (cite a theorem from the course), and find the number of elements in K.

(d) Let $\alpha = \bar{x}$ be the congruence class of x in K. Show that α is a multiplicative generator of the group of units of K.

Hint: In (b), it is not enough to check that the polynomial has no roots in $\mathbb{F}_2$, because the degree is > 3. You have to check for quadratic factors, and (a) might be useful for this purpose. In (c), use Corollary 12.9. In (d), you have to compute powers of $\bar{x}$ in K and check that you obtain all 15 nonzero elements as powers of $\bar{x}$.

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 $n \in \mathbb{N}^+$.

Proof:

(a) Let K be a field of p^n elements of characteristic q, where q is a prime, and consider the additive group $(K, +, 0)$. Then $q \cdot 1 = 0$ in K, but the order of an element divides the order of the group, and therefore $q \mid p^n$. Since q and p are primes, $q = p$.

(b) Let $\phi : \mathbb{Z} \to K$ be the unique homomorphism. Since the characteristic of K is p, it induces an injective homomorphism $\bar{\phi} : \mathbb{Z}/p\mathbb{Z} \to K$. Since $|K| = p$, $\bar{\phi}$ is an isomorphism, and we have $K \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

(c) See (b): $\phi : \mathbb{Z}/p\mathbb{Z} \to K$ is an injective homomorphism with the image isomorphic to $\mathbb{F}_p$.

(d) K contains $\mathbb{F}_p$ as a subfield and can be viewed as a finite dimensional vector space over $\mathbb{F}_p$.

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.*

Proof: Let $f(x) = p(x)q(x)$, where $p(x)$ is irreducible. If $\deg(p(x)) = 1$, then $p(x) = ax + b$ and its root $-\frac{b}{a} \in F$. Suppose that $\deg(p(x)) \geq 2$. Then $K_1 = F[x]/(p(x))$ is a field that contains a root of $p(x)$, given by the congruence class of x in $F[x]/(p(x))$:

$$\overline{p(x)} = p(\overline{x}) = \overline{0} \in \mathbb{K}_1.$$

Denote $\xi = \bar{x} \in K$. Then $f(x) = (x - \xi)g(x)$ in K_1 with $\deg(g) < \deg(f)$. Continue by induction.

Definition 13.3. The smallest field containing all the roots of a polynomial $f(x) \in F[x]$ is called the splitting field of $f(x)$ over F.

Example 13.4. The splitting field of the polynomial $x^2 + 1$ over $\mathbb{R}$ is $\mathbb{C}$.

Proposition 13.5. *The group of units of a finite field K is cyclic.*

Proof: Let $|K^*| = n$ and let m be the maximal order of an element of K^*. Then $m \leq n$. Since K^* is a finite abelian group, the theorem of decomposition into a direct product of cyclic groups applies, in particular $K^* \simeq C_{d_1} \times \ldots \times C_{d_s}$ with $d_1 \mid \ldots \mid d_s$, and $m = d_s$. Then $t^m = 1$ for every $t \in K^*$. The number of roots of a polynomial of degree m in the field K is less or equal to m (suppose $a \in K$ is a root of $f(x)$ of degree $m \geq 1$, then by the Euclidean division we can write $f(x) = (x-a)q(x) + r$ with $r \in K$, therefore $r = 0$ and $f(x) = (x-a)q(x)$ with $\deg(q(x)) = \deg(f(x)) - 1$, proceed by induction). The polynomial $t^m - 1 = 0$ has n distinct roots in K, therefore $n \leq m$ and finally $m = n$.

Example 13.6. The statement that a polynomial of degree n has no more than n distinct roots does not necessarily hold in $A[x]$ where A is not a field. Consider for example $A = \mathbb{Z}/8\mathbb{Z}$ and the polynomial $f(x) = x^2 - 1 \in A[x]$. It has 4 solutions in $\mathbb{Z}/8\mathbb{Z}$: $\{[1]_8, [3]_8, [5]_8, [7]_8\}$. In this case we cannot carry out the proof of Proposition 13.5, and in fact the group of units is not cyclic. We can check that the group of units $(\mathbb{Z}/8\mathbb{Z})^*$ is isomorphic to $C_2 \times C_2$.

Exercise 13.7. Let $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ as in Exercise 12.10. Find a generator of the cyclic group of units of the field $\mathbb{F}_2[x]/(f(x))$.

Theorem 13.8. *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 $K \simeq \mathbb{F}_p[x]/(f(x)) \simeq \mathbb{F}_p[x]/(g(x))$.*

Idea of the proof: K can be constructed as a splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{F}_p$. It can be shown that $K \supset \mathbb{F}_p$ has exactly p^n elements (the derivative of $X^{p^n} - X$ is $p^n X^{p^n - 1} - 1 \cong -1$ modulo p, it has no roots, and therefore the polynomial has no multiple roots). The set K of all roots of $X^{p^n} - X$ forms a field. Indeed, if $a, b \in K$, then $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$ over $\mathbb{F}_p$, same with products and inverses. This proves the existence of a field of p^n elements. Let $L = \mathbb{F}_p/(f(x))$ be another field of p^n elements, where $f(x)$ is an irreducible polynomial of degree n. Then we know that the group of units of L is cyclic of order $p^n - 1$. Let $\alpha \in L^*$ be the generator of the cyclic group of units of L. Then $\alpha^{p^n - 1} = 1$ for all elements of L^*. Adding zero, we have that all elements of L satisfy $\alpha^{p^n} - \alpha = 0$, just like the elements of K. So L is also the splitting field of the same polynomials $X^{p^n} - X$ over $\mathbb{F}_p$. Then we must have $L = \mathbb{F}_p[x]/(f(x)) \simeq K$.

Example 13.9. Check that $g(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ is irreducible. Let $f(x) = x^3 + x + 1$ as in Exercise 12.10. Then we have $\mathbb{F}_2[x]/(f(x)) \simeq \mathbb{F}_2[x]/(g(x))$.

Corollary 13.10. *For any $n \in \mathbb{N}^+$ and any prime p there is an irreducible polynomial $f(x)$ of degree n over $\mathbb{F}_p$.*

Remark 13.11. The corollary fails in fields of characteristic 0.

1. The only irreducible polynomials in $\mathbb{R}[x]$ are of degree 1 and 2.
2. The only irreducible polynomials in $\mathbb{C}[x]$ are of degree 1. A field satisfying this property is called algebraically closed.
3. However, $\mathbb{Q}[x]$ contains irreducible polynomials of any degree $n \geq 1$. Examples can be constructed using the Eisenstein criterion.

Example 13.12. Let $q = p^n$ for a prime number p and an integer $n > 1$, and let $\mathbb{F}_q$ be the unique field of $q = p^n$ elements. Then it is obvious (but good to remember) that $\mathbb{F}_q$ is not isomorphic to the quotient ring $\mathbb{Z}/q\mathbb{Z}$. For example, the ring $\mathbb{Z}/q\mathbb{Z}$ contains zero divisors: $\overline{p^t} \cdot \overline{p^s} = \overline{0} \in \mathbb{Z}/q\mathbb{Z}$, where $s + t = n$. Also, the characteristic of $\mathbb{Z}/q\mathbb{Z}$ is q and the characteristic of $\mathbb{F}_q$ is p.