COURSE 4

Preparing the tools

Integral domains, units

A set R endowed with two binary operations $+$ and $\cdot$ is a **commutative ring** if $(R,+)$ is an Abelian group, $(R,\cdot)$ is a commutative monoid and $\cdot$ is distributive with respect to $+$. A non-zero commutative ring $(R,+,\cdot)$ is an **integral domain** if it has no zero divisors.

Remark 1. In an integral domain R,

$$a,b\in R,\ ab=0\ \Rightarrow\ a=0 \text{ or } b=0.$$

It is important for the multiplicative monoid $(R,\cdot)$ of an integral domain $(R,+,\cdot)$ that one can simplify with any non-zero element. More precisely, for any $a,x,y\in R$, with $a\neq 0$, we have

$$ax=ay\Leftrightarrow a(x-y)=ax-ay=0\overset{a\neq 0}{\Longrightarrow} x-y=0\Rightarrow x=y.$$

An element $a\in R$ of a commutative ring R is a **unit** if there exists $x^{-1}\in R$ such that $xx^{-1}=1$. A non-zero commutative ring is a **field** if all its non-zero elements are units. Obviously, *any field is an integral domain.*

Next, we denote by $U(R)$ **the set of the units of the ring** R.

Remark 2. The set $U(R)=\{x\in R\mid \exists x^{-1}\in R: xx^{-1}=1\}$ is closed in $(R,\cdot)$ and, with the operation induced by $\cdot$, $(U(R),\cdot)$ is a (commutative) group.

Examples 3. a) The ring of intergers $(\mathbb{Z},+,\cdot)$ is an integral domain which is not a field. Its units are -1 and 1.
b) The sets $\mathbb{Q},\mathbb{R},\mathbb{C}$ are fields with the usual addition and multiplication. If K is a field (particularly, if K is one of the above number fields), then $U(K)=K\setminus\{0\}=K^*$.
c) Let R be a commutative ring and let

$$R[X]=\{f=a_0+a_1X+\cdots+a_nX^n\mid a_0,a_1,\dots,a_n\in R,\ n\in\mathbb{N}\}$$

be the set of the polynomials in X over R. The polynomial addition and polynomial multiplication make $(R[X],+,\cdot)$ a commutative ring which includes R and $U(R)\subseteq U(R[X])$.
d) If $d\in\mathbb{Z}\setminus\{1\}$ is a square-free integer then $\mathbb{Z}[\sqrt{d}\,]=\{a+b\sqrt{d}\mid a,b\in\mathbb{Z}\}$ is an integral domain with the usual number addition and multiplication. Indeed, since $0,1\in\mathbb{Z}[\sqrt{d}\,]$ and for any $z_1=a_1+b_1\sqrt{d}$ and $z_2=a_2+b_2\sqrt{d}$ with $a_1,a_2,b_1,b_2\in\mathbb{Z}$ we have

$$z_1-z_2=(a_1-a_2)+(b_1-b_2)\sqrt{d}\in\mathbb{Z}[\sqrt{d}\,],$$

and

$$z_1z_2=(a_1a_2+b_1b_2d)+(a_1b_2+a_2b_1)\sqrt{d}\in\mathbb{Z}[\sqrt{d}\,],$$

$\mathbb{Z}[\sqrt{d}\,]$ is a subring of the field $(\mathbb{C},+,\cdot)$. Thus $\mathbb{Z}[\sqrt{d}\,]$ is a non-zero commutative ring with no zero divisors, i.e. it is an integral domain.

If $d<0$ one considers $\sqrt{d}=i\sqrt{|d|}$ and $\mathbb{Z}[\sqrt{d}\,]=\mathbb{Z}[i\sqrt{|d|}\,]=\{a+bi\sqrt{|d|}\mid a,b\in\mathbb{Z}\}$. In particular, $\mathbb{Z}[-1]=\mathbb{Z}[i]=\{a+bi\mid a,b\in\mathbb{Z}\}$ is **the ring of Gaussian integers**.

e) If $d \in \mathbb{Z} \setminus \{1\}$ is a square-free integer then $\mathbb{Q}(\sqrt{d}\,) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ is a field with the usual number addition and multiplication. Obviously, $0, 1 \in \mathbb{Q}(\sqrt{d}\,)$, and one can prove as in the case of $\mathbb{Z}[\sqrt{d}\,]$ that $z_1 - z_2, z_1 z_2 \in \mathbb{Q}(\sqrt{d}\,)$ for all $z_1, z_2 \in \mathbb{Q}(\sqrt{d}\,)$.

Let $z = a + b\sqrt{d}$ (with $a, b \in \mathbb{Q}$) be a non-zero element from $\mathbb{Q}(\sqrt{d}\,)$. Let us remark that from $\sqrt{d} \notin \mathbb{Q}$ (see the end of the previous course) one deduces that

$$a + b\sqrt{d} = 0 \Leftrightarrow a^2 - b^2 d = 0 \Leftrightarrow a = b = 0.$$

Indeed,

$$a + b\sqrt{d} = 0 \Rightarrow a^2 - b^2 d = (a + b\sqrt{d})(a - b\sqrt{d}) = 0,$$

$$a = b = 0 \Rightarrow a + b\sqrt{d} = 0,$$

and if $a^2 - b^2 d = (a + b\sqrt{d})(a - b\sqrt{d}) = 0$ in $\mathbb{C}$ and $b \neq 0$ then either $\sqrt{d} = \dfrac{a}{b} \in \mathbb{Q}$, or $\sqrt{d} = -\dfrac{a}{b} \in \mathbb{Q}$, which is not possible. Thus also,

$$a^2 - b^2 d = 0 \Rightarrow b = 0 \text{ and (consequently) } a = 0.$$

Now, if we compute the inverse of $z = a + b\sqrt{d} \neq 0$ in $\mathbb{C}$, we obtain

$$z^{-1} = \frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{(a + b\sqrt{d})(a - b\sqrt{d})} = \frac{a - b\sqrt{d}}{a^2 - b^2 d} = \frac{a}{a^2 - b^2 d} + \frac{-b}{a^2 - b^2 d}\sqrt{d} \in \mathbb{Q}(\sqrt{d}\,).$$

Therefore, $\mathbb{Q}(\sqrt{d}\,)$ is a subfield of $(\mathbb{C}, +, \cdot)$, hence $\mathbb{Q}(\sqrt{d}\,, +, \cdot)$ is a field.

f) Let $n \in \mathbb{N},\ n \geq 2$. If $b \in \mathbb{Z}$ we denote

$$\widehat{b} = b + n\mathbb{Z} = \{b + nk \mid k \in \mathbb{Z}\}.$$

By the Division Algorithm, it follows that for any $b \in \mathbb{Z}$ there exists a unique $i \in \{0, 1, \ldots, n-1\}$ such that $\widehat{b} = \widehat{i}$ (i is the remainder of b when divided bty n). Of course, the existence of the remainder from the Division Algorithm implies $\widehat{0} \cup \widehat{1} \cup \cdots \cup \widehat{n-1} = \mathbb{Z}$ and from the uniqueness of the remainder we deduce that $\widehat{i} \cap \widehat{j} = \emptyset$ for any $i, j \in \{0, 1, \ldots, n-1\}$ with $i \neq j$. Thus the classes $\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}$ form a partition of $\mathbb{Z}$ which corresponds to the equivalence relation

$$a \equiv b (\bmod n) \Leftrightarrow n \mid b - a$$

called **congruence modulo** n. Indeed, for any $a, b \in \mathbb{Z}$,

$$\widehat{a} = \widehat{b} \Leftrightarrow a \text{ and } b \text{ give the same remainder when divided by } n \Leftrightarrow n \mid b - a \Leftrightarrow a \equiv b (\bmod n).$$

If we denote $\mathbb{Z}_n = \{\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}\}$, then the operations

$$\widehat{a} + \widehat{b} = \widehat{a+b},\ \widehat{a} \cdot \widehat{b} = \widehat{a \cdot b}$$

are well-defined on $\mathbb{Z}_n$, since for any $a' \in \widehat{a}$ and $b' \in \widehat{b}$, there exist $k_1, k_2 \in \mathbb{Z}$ such that $a' = a + nk_1$ and $b' = b + nk_2$ and we have

$$a' + b' = (a + b) + n(k_1 + k_2) \in \widehat{a+b} \text{ and } a'b' = ab + n(nk_1k_2 + ak_2 + bk_1) \in \widehat{ab}.$$

From the definitions of the operations in $\mathbb{Z}_n$ and the properties of the addition and multiplication in $\mathbb{Z}$ one can easily deduce that $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring, called **the residue class ring**. Its additive identity element is $\widehat{0}$ and $\widehat{1}$ is its multiplicative identity element.

Depending on n, the ring $(\mathbb{Z}_n, +, \cdot)$ may have or may have not zero divisors. For instance, in $\mathbb{Z}_4$, $\widehat{2}$ is a zero divisor since $\widehat{2} \cdot \widehat{2} = \widehat{4} = \widehat{0}$, even if $\widehat{2} \neq \widehat{0}$. But $(\mathbb{Z}_2, +, \cdot)$ is a field since $\mathbb{Z}_2 \setminus \{\widehat{0}\} = \{\widehat{1}\}$ and $\widehat{1}$ is a unit.

A necessary tool for our future work is the degree of a polynomial. Let R be a commutative ring. Any non-zero polynomial f from $R[X]$ can be uniquely written as

$$f = a_0 + a_1X + \cdots + a_nX^n,\ a_0, a_1, \ldots, a_n \in R,\ a_n \neq 0.$$

Under these circumstances, **the degree of** f is the number $n \in \mathbb{N}$ (we write $\deg f = n$). By definition, **the degree of the zero polynomial** 0 is $-\infty$. One notices that the degree 0 polynomials are the non-zero elements of R. Naturally extendingthe addition and the the order relation from $\mathbb{N}$ to $\mathbb{N} \cup \{-\infty\}$, it follows that the degree of a polynomial defines a mapping $\deg : R[X] \to \mathbb{N} \cup \{-\infty\}$ which has the following properties:
1) $\deg(f + g) \leq \max\{\deg f, \deg g\},\ \forall f, g \in R[X]$.
2) $\deg(fg) \leq \deg f + \deg g,\ \forall f, g \in R[X]$.
3) If R is an integral domain, then

$$\deg(fg) = \deg f + \deg g,\ \forall f, g \in R[X].$$

Exercise 1. Show that for an integral domain R, the ring $R[X]$ is also an integral domain and $U(R[X]) = U(R)$.
Solution: Since $\deg(fg) = \deg f + \deg g$, for any $f, g \in R[X]$,

$$fg = 0 \Rightarrow -\infty = \deg(fg) = \deg f + \deg g \Rightarrow \deg f = -\infty \text{ or } \deg g = -\infty \Leftrightarrow f = 0 \text{ or } g = 0,$$

hence $R[X]$ has no zero divisors, the only missing condition to conclude that $R[X]$ is an integral domain.

As we already saw, $U(R) \subseteq U(R[X])$. Let f be a unit in $R[X]$. Since

$$fg = 1 \Rightarrow 0 = \deg(fg) = \deg f + \deg g \Rightarrow \deg f = \deg g = 0 \Leftrightarrow f, g \in R^*,$$

$fg = 1$ in R^*, g is the inverse of f in R, hence f is a unit in R. Thus $U(R[X]) \subseteq U(R)$.

Remark 4. If K is a field, then $U(K[X]) = K^*$, thus $K[X]$ is another example of integral domain which is not a field.

Exercise 2. Let $d \in \mathbb{Z} \setminus \{1\}$ be a square-free integer. If $a, b \in \mathbb{Q}$ and $z = a + b\sqrt{d} \in \mathbb{C}$ then the number $\overline{z} = a - b\sqrt{d}$ is called **the conjugate of** z. Show that:
a) the correspondence $z \mapsto |z \cdot \overline{z}|$ defines a mapping from $\mathbb{Z}[\sqrt{d}\,]$ into $\mathbb{N}$ (we refer to as **the norm map**);
b) the map $\delta : \mathbb{Z}[\sqrt{d}\,] \to \mathbb{N}$, $\delta(z) = |z \cdot \overline{z}|$ has the following properties:
  i) $\delta(z_1z_2) = \delta(z_1)\delta(z_2)$ for all $z_1, z_2 \in \mathbb{Z}[\sqrt{d}\,]$;
  ii) $\delta(z) = 0$ ($z \in \mathbb{Z}[\sqrt{d}\,]$) if and only if $z = 0$;
  iii) $z \in \mathbb{Z}[\sqrt{d}\,]$ is a unit in $\mathbb{Z}[\sqrt{d}\,]$ if and only if $\delta(z) = 1$;
c) the statements i) and ii) from b) are also valid for the map

$$\delta_0 : \mathbb{Q}(\sqrt{d}\,) \to \mathbb{Q},\ \delta_0(z) = |z \cdot \overline{z}|.$$

Solution: a) If $a, b \in \mathbb{Z}$ and $z = a + b\sqrt{d}$, then $\delta(z) = |a^2 - b^2d| \in \mathbb{N}$.
b)i) $\delta(z_1z_2) = |z_1z_2\overline{z_1z_2}| = |z_1z_2\overline{z_1}\,\overline{z_2}| = |z_1\overline{z_1}||z_2\overline{z_2}| = \delta(z_1)\delta(z_2)$, for any $z_1, z_2 \in \mathbb{Z}[\sqrt{d}\,]$.
ii) From the example **3** e) one deduces that for any $a, b \in \mathbb{Z}$,

$$z = a + b\sqrt{d} = 0 \Leftrightarrow a^2 - b^2d = 0 \Leftrightarrow \delta(z) = |a^2 - b^2d| = 0.$$

iii) If z is a unit and z^{-1} is the inverse of z then $\delta(z)\delta(z^{-1}) = \delta(zz^{-1}) = \delta(1) = 1$ in $\mathbb{N}$, and this implies $\delta(z) = 1$. Conversely, if $\delta(z) = |z\overline{z}| = 1$ then $z\overline{z} = \pm 1$, hence z is a unit and its inverse is either $\overline{z}$ or $-\overline{z}$.

c) The solution is very similar to the proof of b)i) and b)ii).

Exercise 3. Show that:
a) For any square-free integer $d \geq 2$, the set uf the units of

$$\mathbb{Z}[\sqrt{-d}\,] = \mathbb{Z}[i\sqrt{d}\,] = \{a + bi\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

is $U(\mathbb{Z}[i\sqrt{d}\,]) = \{-1, 1\}$.
b) The units of the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ are $-1, 1, -i, i$.
c) The ring $\mathbb{Z}[\sqrt{2}]$ has infinitely many units.

Solution: a) Let us consider $z = a + bi\sqrt{d}$ with $a, b \in \mathbb{Z}$. If z is a unit in $\mathbb{Z}[\sqrt{d}]$ then

$$\delta(z) = a^2 + db^2 = 1.$$

Therefore, the natural number a^2 is at most 1, hence we have to study the cases $a^2 = 1$ and $a^2 = 0$. It follows that $(a, b) \in \{(1, 0), (-1, 0)\}$, hence $z \in \{1, -1\}$. Conversely, if $z \in \{1, -1\}$ then it is obviously a unit. In conclusion, $U(\mathbb{Z}[\sqrt{d}]) = \{1, -1\}$.
b) Let $z = a + bi$ be a Gaussian integer $(a, b \in \mathbb{Z})$. We compute the norm of z, and we obtain $\delta(z) = a^2 + b^2$. Therefore z is a unit if and only if $a^2 + b^2 = 1$. Then a^2 is at most 1, hence we have to study the cases $a^2 = 1$ and $a^2 = 0$. It follows that $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$ and this is equivalent to $z \in \{1, -1, i, -i\}$.
c) The sequence $u_n = (1 + \sqrt{2})^n$, $n \in \mathbb{N}$, is an infinite sequence of elements from $\mathbb{Z}[\sqrt{2}]$ which verify the condition b) iii) from the previous exercise.

Exercise 4. Let $n \in \mathbb{N}$, $n \geq 2$. For a non-zero class $\widehat{a} \in \mathbb{Z}_n$ the following conditions are equivalent:
a) $\widehat{a}$ is not a zero divizor in the ring $(\mathbb{Z}_n, +, \cdot)$;
b) $\widehat{a}$ is a unit in the ring $(\mathbb{Z}_n, +, \cdot)$;
c) the integers a and n are coprime integers.

Solution: b)⇒a) Multiplying the equality $\widehat{a}\widehat{b} = \widehat{0}$ with the inverse of $\widehat{a}$, one deduces $\widehat{b} = \widehat{0}$.
a)⇒b) Given a non-zero divisor $\widehat{a} \in \mathbb{Z}_n$, $\widehat{b_1}, \widehat{b_2} \in \mathbb{Z}_n$,

$$\widehat{a} \cdot \widehat{b_1} = \widehat{a} \cdot \widehat{b_2} \Rightarrow \widehat{a} \cdot (\widehat{b_1} - \widehat{b_2}) = \widehat{0} \Rightarrow \widehat{b_1} - \widehat{b_2} = \widehat{0} \Rightarrow \widehat{b_1} = \widehat{b_2}.$$

Thus the correspondence $\mathbb{Z}_n \to \mathbb{Z}_n$, $\widehat{b} \mapsto \widehat{a} \cdot \widehat{b}$ is injective. Since $\mathbb{Z}_n$ is finite, it is also surjective, hence there exists $\widehat{c} \in \mathbb{Z}$ such that $\widehat{a} \cdot \widehat{c} = \widehat{1}$.
b)⇒c) If there exists $\widehat{c} \in \mathbb{Z}$ such that $\widehat{a} \cdot \widehat{c} = \widehat{1}$ (i.e. $\widehat{a \cdot c} = \widehat{1}$) then $n | 1 - ac$, hence there exists $k \in \mathbb{Z}$ such that $1 = kn + ca$, thus $(n, a) = 1$.
c)⇒b) If $(a, n) = 1$ then there exist $k, c \in \mathbb{Z}$ such that $ca + kn = 1$. Then $\widehat{1} = \widehat{ca + nk} = \widehat{ca} + \widehat{nk} = \widehat{c} \cdot \widehat{a} + \widehat{0} = \widehat{c} \cdot \widehat{a}$, hence $\widehat{a} \in U(\mathbb{Z}_n)$ and $\widehat{a}^{-1} = \widehat{c}$.

Remarks 5. a) The equivalence a)⇔b) can be proved in any non-zero finite (unital) ring, therefore *any finite integral domain is a field.*

b) Let $n \in \mathbb{N},\ n \geq 2$. Since in the ring $(\mathbb{Z}_n, +, \cdot)$ the elements which are not zero divisors are exactly the units, $(\mathbb{Z}_n, +, \cdot)$ *is an integral domain if and only if* $(\mathbb{Z}_n, +, \cdot)$ *is a field.* But this happens if and only if $\widehat{1}, \widehat{2}, \dots, \widehat{n-1}$ are units, or, equivalently, if

$$(1, n) = (2, n) = \cdots = (n-1, n) = 1.$$

One can easily notice that under these circumstances, the only natural numbers that divide n are 1 and n, thus $(\mathbb{Z}_n, +, \cdot)$ *is a field if and only if n is a prime number.*

Ideals, principal ideals

Let $(R, +, \cdot)$ be a commutative ring and $I \subseteq R$. On says that I is an **ideal of** R if it fulfils the following conditions:

1) $I \neq \emptyset$
2) if $x, y \in I$ then $x + y \in I$;
3) if $a \in R$ and $x \in I$ then $xa \in I$.

Actually, any ideal of R is a subring, thus it contains the zero element of R. This is how we check 1) most of the time.

Remarks 6. a) In the ideal definition of a (gebneral) ring, one may find instead of 2) the condition
2') if $x, y \in I$ then $x - y \in I$,
since we want I to be a subgroup of $(R, +)$. Since all our rings are unital rings, for any $x \in I$, we have $-x = x \cdot (-1) \in I$, so the conditions 1), 2'), 3) are equivalent to 1), 2), 3).
b) Any ideal of R is a subring R.

Proposition 7. For a commutative ring R, the following statements hold:
i) $0 = \{0\}$ and R ar ideals of R.
ii) If I is an ideal of R which contains a unit of R then $I = R$.
iii) If I and J are ideals then $I \cap J$ is also an ideal.
iv) If I and J are ideals then $I + J = \{x + y \mid x \in I,\ y \in J\}$ is also an ideal.
v) If $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \dots,\ n \in \mathbb{N}^*$, is an ascending chain of ideals then $\bigcup_{n \in \mathbb{N}^*} I_n$ is an ideal.
vi) If $a_1, \dots, a_n \in R$ then

$$(a_1, \dots, a_n) \overset{\text{not}}{=} \{a_1 x_1 + \cdots + a_n x_n \mid x_1, \dots, x_n \in R\}$$

is the smallest ideal of R (with respect to set inclusion) which contains $a_1, \dots, a_n$.

Proof. i) is obvious.
ii) If there exists a unit u of R such that $u \in I$, then for any $a \in R$, thus

$$a = 1 \cdot a = (uu^{-1})a = u(u^{-1}a) \in I,$$

since $u^{-1}a \in R$ and $u \in I$. Thus $R = I$.
iii) $0 \in I$ and $0 \in J$ implies $0 \in I \cap J$.
If $x, y \in I \cap J$ then $x, y \in I$ and $x, y \in J$, therefore $x + y \in I$ and $x + y \in J$, thus $x + y \in I \cap J$.
If $a \in R$ and $x \in I \cap J$ then $xa \in I$ and $xa \in J$, thus $xa \in I \cap J$.
iv) $0 \in I$ and $0 \in J$ implies $0 = 0 + 0 \in I + J$.
If $b, b' \in I + J$ there exist $x, x' \in I$ and $y, y' \in J$ such that $b = x + y$ and $b' = x' + y'$. Since

$$b + b' = (x + y) + (x' + y') = (x + x') + (y + y')$$

and $x+x' \in I$ and $y+y' \in J$, we have $b+b' \in I+J$.

If $a \in R$ and $b \in I+J$ then there exist $x \in I$ and $y \in J$ such that $b = x+y$. Since $xa \in I$ and $ya \in J$, we have $ba = (x+y)a = xa + ya \in I+J$.

v) Obviously, $0 \in \bigcup_{n\in\mathbb{N}^*} I_n$.

Let $x, y \in \bigcup_{n\in\mathbb{N}^*} I_n$. Then there exist $i, j \in \mathbb{N}^*$ such that $x \in I_i$ and $y \in I_j$. If $k = max\{i,j\}$ then $k \in \mathbb{N}^*$, $x \in I_i \subseteq I_k$ and $y \in I_j \subseteq I_k$. Therefore $x+y \in I_k \subseteq \bigcup_{n\in\mathbb{N}^*} I_n$.

If $a \in R$ then $xa \in I_i \subseteq \bigcup_{n\in\mathbb{N}^*} I_n$.

vi) Obviously, $a_i = a_1 \cdot 0 + \cdots + a_{i-1} \cdot 0 + a_i \cdot 1 + a_{i+1} \cdot 0 + \cdots + a_n \cdot 0 \in (a_1, \ldots, a_n)$, for each $i = 1, \ldots, n$. This also implies $(a_1, \ldots, a_n) \neq \emptyset$.

Let $b, b' \in (a_1, \ldots, a_n)$ and $a \in R$. Then there exist $x_1, \ldots, x_n, x_1', \ldots, x_n' \in R$ such that $b = a_1x_1 + \cdots + a_nx_n$ and $b' = a_1x_1' + \cdots + a_nx_n'$. Hence

$$b + b' = (a_1x_1 + \cdots + a_nx_n) + (a_1x_1' + \cdots + a_nx_n') = a_1(x_1 + x_1') \cdots + a_n(x_n + x_n') \in (a_1, \ldots, a_n),$$

$$ba = (a_1x_1 + \cdots + a_nx_n)a = a_1(x_1a) + \cdots + a_n(x_na) \in (a_1, \ldots, a_n).$$

Finally, if I is another ideal of R which contains $a_1, \ldots, a_n$, then for any $b \in (a_1, \ldots, a_n)$, there exist $x_1, \ldots, x_n \in R$ such that $b = a_1x_1 + \cdots + a_nx_n$. Since for each $i = 1, \ldots, n$, $a_ix_i \in I$ we have $b = a_1x_1 + \cdots + a_nx_n \in I$. Thus $(a_1, \ldots, a_n) \subseteq I$. □

The ideal $(a_1, \ldots, a_n)$ is called **the ideal of R generated by** $a_1, \ldots, a_n$. In particular, the ideal $(a) = \{ax \mid x \in R\} \overset{not}{=} aR$ is called **the principal ideal of R generated** by $a \in R$, and

$$(a_1, \ldots, a_n) = a_1R + \cdots + a_nR.$$

Definitions 8. Let R be a commutative ring. An ideal I of R is called **principal ideal** if there exists $a \in R$ such that $I = (a) = aR$. If R is an integral domain and all its ideals are principal ideals, R is called **principal ideal domain** (abreviated **PID**).

Exercise 5. Show that the set of the ideals of the ring of integers $(\mathbb{Z}, +, \cdot)$ is $\{n\mathbb{Z} \mid n \in \mathbb{N}\}$.

Solution 1: First, let us check that for any $n \in \mathbb{N}$, $n\mathbb{Z}$ is an ideal of $(\mathbb{Z}, +, \cdot)$. Of course, $0 = n{\cdot}0 \in n\mathbb{Z}$.

For any $a \in \mathbb{Z}$ and $x, y \in n\mathbb{Z}$, there exist $k, l \in \mathbb{Z}$ such that $x = nk$ and $y = nl$. Therefore $x + y = n(k+l) \in n\mathbb{Z}$ and $xa = n(ka) \in n\mathbb{Z}$.

Conversely, let I be an ideal of $\mathbb{Z}$. We plan to find a natural nuber n such that $I = n\mathbb{Z}$. If $I = \{0\}$ then $n = 0$, otherwise I has at least a nonzero element x. Since also $-x \in I$ either x or x is a nonzero natural number, we have $I \cap \mathbb{N}^* \neq \emptyset$, therefore there exsts a minimum

$$n = \min(I \cap \mathbb{N}^*).$$

We will see that $I = n\mathbb{Z}$. Clearly, for any $k \in \mathbb{Z}$, $n \in I$ implies $nk \in I$. Thus $I \supseteq n\mathbb{Z}$.

Conversely, let $x \in I \subseteq \mathbb{Z}$. From the Division Algorithm we deduce the existence of $q, r \in \mathbb{Z}$ such that $x = nq + r$, with $r \in \mathbb{N}$ and $r < n$. Since

$$x, nq \in I \;\Rightarrow\; r = x - nq \in I,$$

thus $r \in I \cap \mathbb{N}$ and $r < n$, so the only possible value of r is $r = 0$. Hence $x = nq \in n\mathbb{Z}$, which complets the proof of $I \subseteq n\mathbb{Z}$ and the solution.

Solution 2: Any ideal of $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Z}, +, \cdot)$ and any subring of $(\mathbb{Z}, +, \cdot)$ is a subgroup of $(\mathbb{Z}, +)$ which is a cyclic group. Thus the subgroups of $(\mathbb{Z}, +)$ are

$$\langle n \rangle = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} = \langle -n \rangle, \; n \in \mathbb{N}.$$

Once we check (as in Solution 1) that each $n\mathbb{Z}$ is an ideal of $(\mathbb{Z}, +, \cdot)$, the solution is complete.

From this exercise one deduces that:

Remark 9. The ring of integers $(\mathbb{Z}, +, \cdot)$ is a principal ideal domain. We have

$$(0) = \{0\} = 0 \cdot \mathbb{Z} \text{ and } (n) = (-n) = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}, \; \forall n \in \mathbb{Z}^*.$$