SUMMARY OF PART I: RINGS, FIELDS AND IDEALS

1. Basics on Rings and Fields

Definition 1.1. *A* **ring** *is a (non-empty) set with two operations:*

$$\begin{array}{rcll} R \times R & \to & R & \\ (a,b) & \mapsto & a+b & \textit{(addition)} \\ (a,b) & \mapsto & a \cdot b & \textit{(multiplication)} \end{array}$$

such that the following holds:

(i) *With respect to addition, R is an abelian group (i.e., there is an identity, an inverse; associativity and commutativity holds);*
(ii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *associativity for multiplication;*
(iii) $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$, $(a+b) \cdot = (a \cdot c) + (b \cdot c)$ *distributivity.*

Note: • R is necessarily non-empty (due to (i): a group has $\geqslant 1$ elements).
• denote (as usual) $(a \cdot b) + c$ by $a \cdot b + c$ ("multiplication comes first");
• denote $a \cdot b$ by ab.

Definition 1.2. *Let R be a ring.*

(1) *If R has an element $\mathbb{1}_R$ such that $a \cdot \mathbb{1}_R = \mathbb{1}_R \cdot a = a$ for all $a \in R$, then $\mathbb{1}_R$ is called a (multiplicative)* **identity** *for R.*
(2) *If $ab = ba$ $\forall a, b \in R$, then R is called* **commutative**.

Example 1.3: (1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are rings (in fact, commutative, with identity).
(2) For $n \geqslant 2$, $\mathbb{Z}_n$ is not only a group, but moreover it can be given the structure of a commutative ring with identity (we denote as usual $\overline{a} = a + n\mathbb{Z}$ for $a \in \mathbb{Z}$).
For any $a, b \in \mathbb{Z}$, the addition is defined by $\overline{a} + \overline{b} = \overline{a+b}$ and the multiplication is defined by $\overline{a} \cdot \overline{b} = \overline{ab}$.
(3) With our definition, $R = \{0\}$ can be viewed as a ring (with the obvious operations $0+0=0$, $0 \cdot 0 = 0$); in fact, it is not only commutative but has a (strange) identity: the zero element.
(4) Matrix rings.
(5) Polynomial rings: let R be a ring and x a variable. Then $R[x]$ becomes a ring, the polynomial ring in one variable with coefficients in R.

Proposition 1.4. *Let R be a ring, and let $a, b \in R$. Then*

(i) $-(-a) = a$;
(ii) $0_R \cdot a = 0_R = a \cdot 0_R$;
(iii) $a \cdot (-b) = (-a) \cdot b = -a \cdot b$; $(-a) \cdot (-b) = ab$;
(iv) *suppose R contains an identity $\mathbb{1}_R$, then*
$(-\mathbb{1}_R) \cdot a = a \cdot (-\mathbb{1}_R) = -a$.

Definition 1.5. *A* **subring** *of a ring R is a subset $S \subset R$ which is a ring with the induced addition and multiplication of R, i.e.*

(i) $0_R \in S$ *(in particular $S \neq \emptyset$);*
(ii) $a, b \in S$ *implies* $a -_R b \in S$ *(here $a -_R b := a +_R (-b)$);*
(iii) $a, b \in S$ *implies* $a \cdot_R b \in S$.

Note: Conditions (i)+(ii) amount to imposing that $(S, +)$ is a subgroup of the abelian group $(R, +)$.

Examples 1.6: 1) For any $n \in \mathbb{N}$, the set $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, together with the inherited addition and multiplication, becomes a subring of $\mathbb{Z}$; it is commutative, and it does not have an identity if $n > 1$.
2) $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$.
3) $\mathbb{R}[x]_1 := \{a + bx \mid a, b \in \mathbb{R}\}$ is *not* a subring of $\mathbb{R}[x]$.
4) $Z[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ (with $i^2 = -1$), the *Gaussian integers*, form a subring of the very special ring $\mathbb{C}$ of complex numbers (in fact, this is a very special ring, called a *field* (see below)).

Definition 1.7. *Let R and S be rings. A* **homomorphism of rings** *from R to S is a map $\varphi : R \to S$ satisfying*
(i) *for any $a, b \in R$ we have* $\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$*;*
(ii) *for any $a, b \in R$ we have* $\varphi(a \cdot_R b) = \varphi(a) \cdot_S \varphi(b)$*;*

Examples 1.8: For $n \geqslant 2$ we know that the reduction map

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}_n \\ a &\mapsto \overline{a} := \{a + kn \mid k \in \mathbb{Z}\} \end{aligned}$$

is a homomorphism *of groups*. It is in fact even a homomorphism *of rings*, since we also have

$$\varphi(a \cdot_{\mathbb{Z}} b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \varphi(a) \cdot_{\mathbb{Z}_n} \varphi(b)\,.$$

Note: Some authors require, in case both R and S have an identity, that a ring homomorphism $\varphi : R \to S$ respect the identity, i.e., $\varphi(\mathbb{1}_R) = \mathbb{1}_S$. This is not guaranteed, as the following example shows: $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_6$, sending $\overline{1}$ to $\overline{3}$ (and $\overline{0}$ necessarily to $\overline{0}$).

Definition 1.9. *Let R and S be rings. A map $\varphi : R \to S$ is a* homomorphism of rings *if it satisfies (i) and (ii), where*
(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$ *for all $a, b \in R$;*
(ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ *for all $a, b \in R$.*

Examples 1.10: 1) The following map is a homomorphism of rings

$$\begin{aligned} \varphi : \mathbb{Z}[i] &\to \mathbb{Z}_2\,, \\ a + ib &\mapsto \overline{a + b}\,. \end{aligned}$$

2) "Specialisation homomorphism": let S be a commutative ring, R a subring of S (necessarily commutative). For any $a \in S$ the map $\varphi_a : R[x] \to S$, sending $f(x)$ to $f(a)$, is a homomorphism of rings.
3) In particular, $\varphi : \mathbb{Z}[x] \to \mathbb{C}$, sending $f(x)$ to $f(i)$, is a homomorphism of rings. (This is far from being surjective; but it is also not injective: take $f(x) = x^2 + 1$.)
4) Let $\varphi : R \to S$ and $\varphi : S \to T$ be ring homomorphisms. Then the composition of the two, $\psi \circ \phi : R \to T$ (note the order), is again a ring homomorphism.

Definition 1.11. (i) *A homomorphism of rings* $\varphi : R \to S$ *is called an* **isomorphism** *if* φ *is both injective and surjective (as a map between sets).*

(ii) *The* **kernel** *and the* **image** *of a homomorphism of rings* $\varphi : R \to S$ *are defined by* $\ker(\varphi) = \{a \in R \mid \varphi(a) = 0_S\} \subset R$ *and* $\operatorname{im}(\varphi) = \{\varphi(a) \mid a \in R\} \subset S$.

Example 1.12: (Example 1.9 revisited) The homomorphism of rings $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_2$, $\varphi(a+ib) = \overline{a+b}$, is surjective ($\varphi(0) = \overline{0}$ and $\varphi(1) = \overline{1}$), but not injective: we compute the obstruction to being injective.

$$\begin{aligned}
\ker(\varphi) &= \{a+ib \in \mathbb{Z}[i] \mid \overline{a+b} = \overline{0} \text{ in } \mathbb{Z}_2\} \\
&= \{a+ib \in \mathbb{Z}[i] \mid a+b = 2k \text{ for some } k \text{ in } \mathbb{Z}\} \\
&\subset \{2k - b + ib \mid b, k \text{ in } \mathbb{Z}\} \\
&= \{\big((-1-i)k + b\big)(-1+i) \mid b, k \text{ in } \mathbb{Z}\} \qquad [\text{use } 2 = (-1-i)(-1+i)] \\
&\subset \{\gamma(-1+i) \mid \gamma \text{ in } \mathbb{Z}[i]\}\,.
\end{aligned}$$

The reverse inclusion $\{\gamma(-1+i) \mid \gamma \in \mathbb{Z}[i]\} \subset \ker(\varphi)$ also holds:

$$\varphi\big(\gamma(-1+i)\big) = \varphi(\gamma)\varphi(-1+i) = \varphi(\gamma) \cdot \overline{0} = \overline{0} \qquad \forall \gamma \in \mathbb{Z}[i]\,.$$

Proposition 1.13. *A ring homomorphism* $\varphi : R \to S$ *is injective* $\Leftrightarrow \ker(\varphi) = \{0_R\}$.

Definition 1.14. *Let* R *be a ring.*

(i) R *is called an* **integral domain** *if* R *is commutative, has an identity* $\mathbb{1}_R \neq 0_R$ *and if for all* $a, b \in R$ *one has*

$$ab = 0_R \;\Rightarrow\; a = 0_R \text{ or } b = 0_R\,.$$

(ii) R *is called a* **field** *if* R *is commutative, has an identity* $\mathbb{1}_R \neq 0_R$, *and if each* $a \in R - \{0_R\}$ *has a multiplicative inverse, i.e.*

$$\forall a \in R - \{0_R\}\ \exists b \in R \ \text{ such that } ab = \mathbb{1}_R = ba\,.$$

Proposition 1.15. (i) *A field is in particular an integral domain.*

(ii) *"Cancellation": let* R *be an integral domain, let* $a, b, c \in R$ *with* $ab = ac$ *and* $a \neq 0_R$. *Then* $b = c$. [*In words: A non-zero* a *can be cancelled.*]

Examples 1.16: 1) $\mathbb{Z}$ is an integral domain, but no field.

2) $\mathbb{Z}[i]$ ($i^2 = -1$) is an integral domain (no field): it is a subring of $\mathbb{C}$ (which is commutative), so it inherits commutativity; furthermore, $\mathbb{1}_{\mathbb{Z}[i]} = 1 + 0 \cdot i \neq 0 + 0 \cdot i = 0_{\mathbb{Z}[i]}$; finally $ab = 0$ implies either $a = 0$ or $b = 0$.

3) The polynomial rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are both integral domains, but no fields.

4) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.

5) $\mathbb{Z}_n$ is a field if (and only if) n is a prime number.

Remark 1.17: In a field F, we can perform "division by a" for any non-zero $a \in F$. Also we can do linear algebra for vector spaces over F: all the familiar notions like dimension, basis, linear (in-)dependence, determinants or invertibility of a matrix make sense.

Example 1.18: In $M_2(\mathbb{R})$, the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has an inverse if and only if its determinant $ad - bc$ is non-zero, in which case its inverse has the form $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Definition 1.19. *Let R be a ring with identity $1 \neq 0$. Then $R^* = \{a \in R \mid \exists b \in R$ such that $ab = ba = 1\}$ is called the set of* **units** *of R.*

Notation. For $a \in R^*$, the (unique!) element $b \in R$ such that $ab = ba = 1$ is denoted by a^{-1}.

Examples 1.20: 1) $\mathbb{Z}^* = \{-1, 1\}$. [Note that this is different from $\mathbb{Z} - \{0\}$.]
2) $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.
3) Let $n \geqslant 2$ be an integer. then $\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$.
4) Let F be a field. Then $F^* = F - \{0\}$.
5) For a field F, the units in $M_n(F)$ (the ring of $(n \times n)$-matrices with coefficients in F) are the elements with non-zero determinant.

Definition 1.21. *Let R be a commutative ring with identity $1 \neq 0$. Then a* **divides** *b, denoted $a \,|\, b$, if and only if $\exists c \in R : ac = b$.*

Example 1.22: In $\mathbb{Z}[i]$ we want to find all elements dividing a given $\gamma \in \mathbb{Z}[i]$. Important tool: the **norm map** $N : \mathbb{Z}[i] \to \mathbb{Z}$, sending $a + bi$ to $a^2 + b^2$. It is multiplicative (i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$) and it transfers divisibility in $\mathbb{Z}[i]$ into divisibility in $\mathbb{Z}$:

$$(\alpha \,|\, \gamma \text{ in } \mathbb{Z}[i]) \Rightarrow (N(\alpha) \,|\, N(\gamma) \text{ in } \mathbb{Z})\,.$$

[The reverse direction does *not* hold in general!]

In this way, the problem is reduced to two simpler problems: 1) to check divisibility in $\mathbb{Z}$ (there are only few candidates α left for which $N(\alpha)$ divides the integer $N(\gamma)$), and 2) to test these candidates one by one whether they indeed can be multiplied by a number in $\mathbb{Z}[i]$ to give that integer $N(\gamma)$.

Note: Divisibility is not changed when we multiply by units: let ε be a unit in the commutative ring R, and α, $\beta \in R$. Then

$$\alpha \,|\, \beta \;\Leftrightarrow\; \varepsilon\alpha \,|\, \beta \;\Leftrightarrow\; \alpha \,|\, \varepsilon\beta\,.$$

2. Polynomial rings over a field

For a field F and a variable x, the elements of $F[x]$ have the form $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ (for some $n \in \mathbb{N} \cup \{0\}$) and $a_i \in F$, $i = 0, \ldots, n$.

Definition 2.1. *The* **degree** $\deg\big(f(x)\big)$ *of a non-zero polynomial $f(x) = a_n x^n + \ldots + a_0 \in F[x]$ with $a_n \neq 0$ is defined as n, the largest index j such that $a_j \neq 0$. We call a_n the* **leading coefficient** *of $f(x)$, and we call $f(x)$* **monic** *if its leading coefficient if equal to 1.*

For $f(x) = 0$, we put $\deg\big(f(x)\big) = -\infty$.

Proposition 2.2. *Let F be a field. Then $F[x]$ is an integral domain, and $\deg\big(f(x)g(x)\big) = \deg\big(f(x)\big) + \deg\big(g(x)\big)$.*

Proposition 2.3. *(Division algorithm)*

Let F be a field and $f(x)$, $g(x) \in F[x]$ with $f(x) \neq 0$.

Then there are unique elements $q(x)$ and $r(x)$ in $F[x]$ with $\deg\big(r(x)\big) < \deg\big(f(x)\big)$ and $g(x) = q(x)f(x) + r(x)$.

Example 2.4: For $f(x) = x^3 + x + 1$ and $g(x) = x^5 + 2x^4 + x^2 + 3$ in $\mathbb{Q}[x]$, we get from dividing $g(x)$ by $f(x)$:

$$g(x) = (x^2 + 2x - 1)f(x) - 2x^2 - x + 4\,,$$

with $q(x) = x^2 + 2x - 1$ and $r(x) = -2x^2 - x + 4$ of degree 2 ($< \deg\big(g(x)\big) = 3$).

Definition 2.5. *Let R be a commutative ring and $f(x) \in R[x]$. An element $a \in R$ is called a* **root** *of $f(x)$ if $f(a) = 0$.*

Example 2.6: In $R = \mathbb{Z}_6$, $f(x) = x^2 + \overline{3}x + \overline{2}$ has 4 roots: $\overline{1}, \overline{2}, \overline{4}$ and $\overline{5}$. (We can write $f(x) = (x + \overline{1})(x + \overline{2}) = (x - \overline{1})(x - \overline{2})$.)

Proposition 2.7. *Let F be a field, $f(x) \in F[x]$ and $a \in F$.*
Then a is a root of $f(x)$ $\Leftrightarrow$ $x - a$ divides $f(x)$ in $F[x]$.

Example 2.8:
1) One of the roots of $x^3 - \overline{1}$ in $\mathbb{Z}_5$ is $\overline{1}$. Dividing it by $x - \overline{1}$ gives $x^3 - \overline{1} = (x - \overline{1})(x^2 + x + \overline{1})$. Since the second factor has no roots in $\mathbb{Z}_5$ (e.g., by trial and error), $\overline{1}$ is a so-called **simple** root of $x^3 - \overline{1}$ in $\mathbb{Z}_5$.
2) One of the roots of $x^3 - \overline{1}$ in $\mathbb{Z}_3$ is also $\overline{1}$, but here we find $x^3 - \overline{1} = (x - \overline{1})(x - \overline{1})(x - \overline{1})$ in $\mathbb{Z}_3[x]$, and $\overline{1}$ is a **multiple** (more precisely, a 3-fold) root of $x^3 - \overline{1}$ in $\mathbb{Z}_3$.

Corollary 2.9. *If F is a field and $f(x) \in F[x]$ is of degree $n \geqslant 1$, then $f(x)$ has at most n roots in F.*

Examples 2.10:
1) (Cf. Example 2.8) $x^3 - \overline{1}$ has only one root in $\mathbb{Z}_5$.
2) $x^2 - 2$ in $\mathbb{Q}[x]$ has no roots in $\mathbb{Q}$ ($\pm\sqrt{2} \notin \mathbb{Q}$).
3) $x^2 - 2$ in $\mathbb{R}[x]$ has two roots ($\pm\sqrt{2} \in \mathbb{R}$).
4) (Cf. Example 2.6) $x^2 + \overline{3}x + \overline{2}$ in $\mathbb{Z}_6[x]$ has four roots (no counterexample to 2.9 since $\mathbb{Z}_6$ is not a field).
5) $x^2 + \overline{3}x + \overline{2}$ in $\mathbb{Z}_5[x]$ has only two roots ($\overline{3}, \overline{4}$) (as it should by 2.9 since $\mathbb{Z}_5$ is a field).

Definition 2.11. *Let F be a field, $f(x)$, $g(x) \in F[x]$. Then $d(x) \in F[x]$ is called a* **greatest common divisor** *of $f(x)$ and $g(x)$ if*
(i) *$d(x) \mid f(x)$ and $d(x) \mid g(x)$ and*
(ii) *any $e(x) \in F[x]$ which divides both $f(x)$ and $g(x)$ also divides $d(x)$.*

Example 2.12: Let $f(x) = x^3 + x^2 + \overline{2}x + \overline{2}$, $g(x) = x^3 + \overline{2}x^2 + x + \overline{2}$ in $\mathbb{Z}_3[x]$. We perform division with remainder:

$$\begin{aligned} g(x) &= \overline{1} \cdot f(x) + (x^2 + \overline{2}x)\,, \\ f(x) &= (x + \overline{2}) \cdot (x^2 + \overline{2}x) + (x + \overline{2})\,, \\ (x + \overline{2}) &= x(x + \overline{2}) + 0\,. \end{aligned} \tag{1}$$

Therefore we have $\gcd\big(f(x), g(x)\big) = x + \overline{2}$. (It is already monic.)

Theorem 2.13. *Let F be a field and $f(x)$, $g(x) \in F[x]$. Then there exists a gcd $d(x)$ of $f(x)$ and $g(x)$. It is unique up to multiplication by elements in F^*.*

If $f(x)$ and $g(x)$ are not both 0, then we can compute a gcd of $f(x)$ and $g(x)$ using the Euclidean algorithm. We can find, using iterated substitution, $A(x)$ and $B(x)$ in $F[x]$ such that $d(x) = A(x)f(x) + B(x)g(x)$.

Example 2.14: (Example 2.12 cont'd) We have seen that $x + \overline{2}$ is a gcd of $f(x) = x^3 + x^2 + \overline{2}x + \overline{2}$ and $g(x) = x^3 + \overline{2}x^2 + x + \overline{2}$ in $\mathbb{Z}_3[x]$. Using the second and the first line in (1), we find

$$x + \overline{2} = f(x) - (x + \overline{2})(x^2 + \overline{2}x) = f(x) - (x + \overline{2})(g(x) - f(x)) = xf(x) - (x + \overline{2})g(x)\,.$$

Definition 2.15. *Let F be a field. Then $f(x)$ in $F[x]$ is called* **irreducible** *if*
1) *$\deg\big(f(x)\big) \geqslant 1$ (i.e., $f(x) \neq 1$ and $f(x)$ is not a unit).*

2) *If $f(x) = g(x) \cdot h(x)$ with $g(x)$ and $h(x)$ in $F[x]$, then $f(x)$ or $g(x)$ is in F^* (i.e., $g(x)$ or $h(x)$ has degree 0).*

Otherwise $f(x)$ is called **reducible**.

$f(x)$ is called **prime** *if, for any $g(x)$, $h(x) \in F[x]$,*

$$f(x) \mid g(x)h(x) \Rightarrow \big(f(x) \mid g(x) \text{ or } f(x) \mid h(x)\big)\,.$$

Example 2.16: Checking irreducibility for general polynomials of small degree:

- $\deg\big(f(x)\big) = 1$. Then $f(x)$ is irreducible.
- $\deg\big(f(x)\big) = 2$. Suppose $f(x) = g(x)h(x)$ in $F[x]$, then $2 = \deg\big(f(x)\big) = \deg\big(g(x)\big) + \deg\big(h(x)\big) = 0 + 2$ or $= 1 + 1$ or $= 2 + 0$. Therefore $f(x)$ is reducible if and only if the second case $1 + 1$ can occur, i.e., if and only if $f(x)$ can be written as a product of two polynomials of degree 1, i.e., if and only if $f(x)$ has a root in F.
- $\deg\big(f(x)\big) = 3$. Suppose $f(x) = g(x)h(x)$ in $F[x]$, then $3 = \deg\big(f(x)\big) = \deg\big(g(x)\big) + \deg\big(h(x)\big) = 0 + 3$ or $= 1 + 2$ or $2 + 1$ or $= 3 + 0$. Therefore $f(x)$ is reducible if and only if one of the two cases $1+2$ or $2+1$ can occur, i.e., if and only if $f(x)$ is divisible by a polynomial of degree 1, i.e., if and only if $f(x)$ has a root in F.
- $\deg\big(f(x)\big) = 4$. $f(x)$ is reducible if and only if one of the three cases $1 + 3$, $2 + 2$ or $3 + 1$ can occur, i.e., if and only if $f(x)$ has a root in F or $f(x)$ is a product of two quadratic factors.

Examples 2.17: Checking irreducibility for specific polynomials of small degree:

1) $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, since $\deg(x^2 + 1) = 2$ and it has no roots in $\mathbb{R}$.
2) $x^2 + 1$ is reducible in $\mathbb{C}[x]$, since it has roots in $\mathbb{C}$ (in fact, $\pm i$).
3) $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, since it is of degree 2 and has no roots in $\mathbb{Q}$.
4) $x^2 - 2$ is reducible in $\mathbb{R}[x]$, since it has roots in $\mathbb{R}$ (in fact, $\pm\sqrt{2}$).
5) $x^3 - 2x + 2$ has odd degree and must therefore have a root in $\mathbb{R}$. Therefore it is reducible in $\mathbb{R}[x]$.
6) $x^3 - 2x + 2$ is irreducible in $\mathbb{Q}[x]$ since it has degree 3 and no root in $\mathbb{Q}$.
7) $x^4 + 2x^2 + 1$ has no roots in $\mathbb{R}$, but it is nevertheless reducible in $\mathbb{R}[x]$ since it factors as $(x^2 + 1)^2$.

Proposition 2.18. *Let $f(x) = a_n x^n + \ldots + a_0$ be in $\mathbb{Z}[x]$ of degree $n \geqslant 1$. If $b/c \in \mathbb{Q}$ is a root of $f(x)$ such that $\gcd(b, c) = 1$, then necessarily $c \mid a_n$ and $b \mid a_0$. In particular, if $a_n = \pm 1$, then all the roots of $f(x)$ in $\mathbb{Q}$ must in fact belong to $\mathbb{Z}$.*

Example 2.19: The roots of $f(x) = x^2 - 2x + 2$ in $\mathbb{Q}$, if they exist, must lie in $\{\pm 1, \pm 2\}$. Substituting shows that none of them is a root. Therefore $f(x)$ has no root in $\mathbb{Q}$ (and since it is furthermore of degree $\leqslant 3$, it is irreducible in $\mathbb{Q}[x]$).

Proposition 2.20. *Let F be a field and $f(x) \in F[x]$ be irreducible. Then $f(x)$ is prime.*

Theorem 2.21. *Let F be a field, and let $f(x)$ be in $F[x]$ of degree at least 1. Then*

- *(Existence) $f(x) = g_1(x) \cdot \cdots \cdot g_s(x)$ for some $g_j(x)$ which are irreducible in $F[x]$;*
- *(Uniqueness) if $f(x) = h_1(x) \cdot \cdots \cdot h_t(x)$ for some $h_j(x)$ which are irreducible in $F[x]$, then necessarily $s = t$ and—after renumbering the $h_j(x)$ if necessary—we have $g_j(x) = c_j \cdot h_j(x)$ for some $c_j \in F^*$.*

Examples 2.22: 1) Let $F = \mathbb{Q}$ and $f(x) = 3x^3+x^2+6x+2 = (x+\frac{1}{3})(3x^2+6)$. The linear (i.e., of degree 1) factor $x + \frac{1}{3}$ is irreducible; but also the second factor $3x^2 + 6$ is irreducible as it has degree 2 and has no root in $\mathbb{Q}$. We have also other decompositions, like $f(x) = (3x+1)(x^2+2)$, whose factors can be written according to the theorem as $c_1(x + \frac{1}{3})$ and $c_2(3x^2 + 6)$ for some $c_j \in \mathbb{Q}^*$ (in fact, we find $c_1 = 3$ and $c_2 = \frac{1}{3}$).

2) Let $f(x) = x^4 + x^3 + 2x^2 + 4x + 2 \in \mathbb{Q}[x]$. Candidate roots are $\pm 1, \pm 2$. A quick check shows that -1 is indeed a root, and $f(x) = (x+1)(x^3+2x+2)$. The second factor is irreducible since it is of degree $\leqslant 3$ and has no root in $\mathbb{Q}$. (The first factor is irreducible, since it is of degree 1.)

3) Let $f(x) = x^4 - 4$ in $\mathbb{Q}[x]$. Then candidate roots are $\pm 1, \pm 2, \pm 4$. A quick check shows that none of them are roots. We cannot yet conclude irreducibility, though, since there is still the possibility that $f(x)$ decomposes into two (necessarily irreducible) quadratic factors—and this indeed holds: $f(x) = (x^2 + 2)(x^2 - 2)$.

4) Let $f(x) = x^3 - \overline{1}$ in $\mathbb{Z}_5[x]$. One checks that $\overline{1}$ is a root, and that the second factor in the decomposition $x^3 - \overline{1} = (x - \overline{1})(x^2 + x + \overline{1})$ is also irreducible (it has no root in $\mathbb{Z}_5$ and is of degree $\leqslant 3$).

Remark 2.23: Let F be a field. If $f(x) \in F[x]$ is of degree at least one, then we could also write $f(x) = c \cdot g_1(x) \cdot \dots \cdot g_k(x)$ with $c \in F^*$ the leading coefficient of $f(x)$, and where all $g_j(x)$ are monic and irreducible in $F[x]$.

This decomposition is unique, up to permutation of the $g_j(x)$.

Lemma 2.24. *Let $f(x)$ be in $\mathbb{Z}[x]$, $n \geqslant 2$ an integer. Then reducing the coefficients modulo n, i.e., the map*

$$\begin{array}{rcl} \varphi_n : \mathbb{Z}[x] & \to & \mathbb{Z}_n[x] \\ f(x) = a_m x^m + \ldots + a_0 & \mapsto & \overline{f}(x) := \overline{a_m} x^m + \ldots + \overline{a_0} \end{array}$$

is a ring homomorphism.

Theorem 2.25. *(Gauss lemma) Let $f(x) \in \mathbb{Z}[x]$ have degree $\geqslant 1$. Suppose $f(x) = g(x)h(x)$ with $g(x)$, $h(x) \in \mathbb{Q}[x]$.*

Then already $f(x) = \widetilde{g}(x)\widetilde{h}(x)$ with $\widetilde{g}(x)$, $\widetilde{h}(x) \in \mathbb{Z}[x]$ and $\deg\big(\widetilde{g}(x)\big) = \deg\big(g(x)\big)$, $\deg\big(\widetilde{h}(x)\big) = \deg\big(h(x)\big)$. *More precisely, there exists an $a \in \mathbb{Q}^*$ such that $a \cdot g(x) \in \mathbb{Z}[x]$ and $a^{-1} \cdot h(x) \in \mathbb{Z}[x]$.*

Examples 2.26: 1) The quadratic polynomial $f(x) = 2x^2+7x+3$ which can be decomposed over $\mathbb{Q}$ as $(x+\frac{1}{2})(2x+6)$ has a decomposition in $\mathbb{Z}[x]$ given by $f(x) = (2x + 1)(x + 3)$.

2) Factorize $x^4 + 4$ in $\mathbb{Q}[x]$. It has no roots in $\mathbb{Q}$, so either it is irreducible or it factorises as a product of two quadratics (without roots in $\mathbb{Q}$).

Make the "Ansatz" $x^4 + 4 = (Ax^2 + Bx + C)(Dx^2 + Ex + F)$ with $A, B, \ldots, F \in \mathbb{Q}$. By the Gauss lemma, we can find a factorisation of the same type with $A, B, \ldots, F \in \mathbb{Z}$.

Multiplying out and comparing coefficients of the different monomials x^r $(r = 0, \ldots, 4)$ gives us conditions on the integers $A, \ldots, F$. A short calculation then gives indeed a factorization

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)\,.$$

Proposition 2.27. *(Criterion for irreducibility in $\mathbb{Z}[x]$)*
Let $f(x) \in \mathbb{Z}[x]$ be non-constant. Let p be a prime number *such that $\overline{f}(x) \in \mathbb{Z}_p[x]$ has the same degree as $f(x)$.*
If $\overline{f}(x)$ is irreducible in $\mathbb{Z}_p[x]$ then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Examples 2.28: 1) $f(x) = 3x^2 + 7x + 13$. Take $p = 2$: $\overline{f}(x) = x^2 + x + \overline{1} \in \mathbb{Z}_2[x]$. The latter is irreducible in $\mathbb{Z}_2[x]$ as it has degree 2 and neither $\overline{0}$ nor $\overline{1}$ are roots. Furthermore $\deg\big(f(x)\big) = \deg\big(\overline{f}(x)\big) = 2$.
Therefore $f(x)$ is irreducible in $\mathbb{Q}[x]$.
2) $f(x) = 3x^2 + 2x$, take $p = 3$. Then $\overline{f}(x) = \overline{2}x$ is irreducible in $\mathbb{Z}_3[x]$, as it has degree 1. But $f(x) = x(3x + 2)$ is *not* irreducible. [Note that $\deg\big(\overline{f}(x)\big) < \deg\big(f(x)\big)$.]

Proposition 2.29. *(Eisenstein's [irreducibility] criterion)*
Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$, $a_n \neq 0$, $n \geq 1$. If there is a prime $p \in \mathbb{Z}$ with

$$p \mid a_0,\ \ p \mid a_1, \ldots, p \mid a_{n-1}\,,\ \ \textit{but } p \nmid a_n \ \textit{and } p^2 \nmid a_0\,,$$

then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Examples 2.30: 1) $f(x) = x^n - 2$, for $n \in \mathbb{N}$, is irreducible in $\mathbb{Q}[x]$, by Eisenstein's criterion for $p = 2$.
2) Let p be prime. Then $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible in $\mathbb{Q}[x]$. [Use: $f(x)$ irreducible $\Leftrightarrow$ $f(x+1)$ irreducible; then, writing $f(x) = \frac{x^p - 1}{x-1}$ gives

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x^p + \binom{p}{1}x^{p-1} + \ldots + \binom{p}{p-1}x + 1) - 1}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \ldots + \binom{p}{p-1}. \end{aligned}$$

Now apply Eisenstein's criterion for the prime p.]

3. Ideals and Quotient Rings

Definition 3.1. *Let R be a ring. A subset I in R is called an* **ideal** *if the following three conditions hold:*

(i) $0_R \in I$;
(ii) *if r and s are in I, then also $r - s \in I$;*
(iii) *if $r \in I$ and $a \in R$, then $r \cdot a \in I$ and $a \cdot r \in I$.*

Note: In particular, I is a subring of R (can think of it as a "black hole": it absorbs everything which comes near it...).

Remark 3.2: If R has an identity $\mathbb{1}_R$, and if an ideal $I \subset R$ contains $\mathbb{1}_R$, then necessarily $I = R$. Similarly, if I contains any unit, then $I = R$.

Examples 3.3: (1) $R = \mathbb{Z}$. Then any subgroup under addition is either $\{0\}$ or of the form $n\mathbb{Z}$ $(n = 1, 2, \ldots)$. All of them are ideals, and any ideal (which is in particular a subgroup) of $\mathbb{Z}$ is of this form. (For $n = 1$ we get the full ring.)
(2) "Trivial ideals": $\{0\}$ is an ideal, R is also an ideal (for any ring R).
(3) $R = F$ a field. Its only ideals are $\{0\}$ and R (any $r \neq 0$ is a unit).

Examples 3.4: 1) $(a) = \{ra \mid r \in R\}$ has a *single* generator and is called a **principal** ideal.

2) $(a_1, a_2) = \{r_1a_1 + r_2a_2 \mid r_1, r_2 \in R\}$. Sometimes this can be written simpler, e.g., $(15, 21)_{\mathbb{Z}} = (3)_{\mathbb{Z}}$.

3) All ideals in $\mathbb{Z}$ are principal (cf. Example 3.3 (1)).

Proposition 3.5. *Let $\varphi : R \to S$ be a ring homomorphism. Then $\ker(\varphi)$ is an ideal.*

Examples 3.6: 1) (Cf. Example 1.11) $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_2$, $\varphi(a + bi) = \overline{a + b}$, is a homomorphism of rings, with $\ker(\varphi) = \{\gamma(-1 + i) \mid \gamma \in \mathbb{Z}[i]\} = (-1 + i)$, a (principal) ideal in $\mathbb{Z}[i]$.

2) $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_{37}$, sending $a + bi$ to $\overline{a + 6b}$, is a ring homomorphism. Since $\overline{6}^2 = -\overline{1}$ in $\mathbb{Z}_{37}$, the number $\overline{6}$ reflects the crucial property of the number i in $\mathbb{Z}[i]$. Then $\ker(\varphi) = (37, 6 - i) = \{\alpha \cdot 37 + \beta(6 - i) \mid \alpha, \beta \in \mathbb{Z}[i]\}$.

Example 3.7: (Example 3.6, 2), revisited) There is a simpler description of the kernel, since $(37, 6 - i) = (6 - i)$ (note that $37 = (6 - i)(6 + i)$ already lies in the ideal $(6 - i)$).

Proposition 3.8. *Let F be a field. Then all ideals of $F[x]$ are principal. More precisely, the ideals of $F[x]$ are given by (0), (1) and $\big(f(x)\big)$ for $\deg\big(f(x)\big) \geqslant 1$.*

Moreover, we have the inclusion of ideals

$$\big(f(x)\big) \subset \big(g(x)\big) \quad \textit{iff} \quad g(x) \mid f(x) \in F[x]$$

and equality of ideals

$$\big(f(x)\big) = \big(g(x)\big) \quad \textit{iff} \quad f(x) = c \cdot g(x) \in F[x] \textit{ for some } c \in F^*.$$

[*In particular, each non-zero ideal of $F[x]$ has a unique* monic *generator.*]

Let R be a ring and $I \subset R$ an ideal. The set of cosets $\{a + I \mid a \in R\}$ not only forms a group, the **quotient group** R/I, but in fact even becomes a ring.

The multiplication of cosets is given, for $a, b \in R$, as

$$(a + I)(b + I) = a \cdot b + I\,.$$

Definition 3.9. *For an ideal I in a ring R, the map $\pi : R \to R/I$, sending $a \in R$ to its coset $a + I$, is called the* **canonical projection** *(along I), and R/I is called the* **quotient ring** *of R with respect to I.*

Proposition 3.10. 1) *R/I is indeed a ring.* [*So the name is justified.*]

2) *The canonical projection $\pi : R \to R/I$ is a ring homomorphism. Morever, it is surjective, and I is its kernel.*

Note: Computation rules in R/I:

- $\overline{a} + \overline{b} = \overline{a + b}$, $\quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$.
- $\overline{a} = \overline{b} \Leftrightarrow a - b \in I$ $\quad$ (in particular $\overline{a} = \overline{0} \Leftrightarrow a \in I$).

Examples 3.11: 1) Let $I = (-1 + i)_{\mathbb{Z}[i]} \subset \mathbb{Z}[i]$. Then $\overline{-6 + i} = \overline{-i}$ in $\mathbb{Z}[i]/I$.

2) Let $I = (x^2 + x + 1)_{\mathbb{Q}[x]} \subset \mathbb{Q}[x]$. Then $\overline{x + 2} \neq \overline{2x^2}$ in $\mathbb{Q}[x]/(x^2 + x + 1)$.

Theorem 3.12. *(First Isomorphism Theorem for Rings) Let $\varphi : R \to S$ be a* **surjective** *ring homomorphism. Then there is an* **isomorphism** *of rings*

$$\begin{aligned} R/\ker(\varphi) &\;\to\; S\,, \\ a + \ker(\varphi) &\;\mapsto\; \varphi(a)\,. \end{aligned}$$

Example 3.13: Define $\varphi : \mathbb{R}[x] \to \mathbb{C}$, sending $f(x)$ to $f(i)$ (where $i^2 = -1$). We can check the following properties.

- φ is a homomorphism of rings.
- φ is surjective: any $a + bi \in \mathbb{C}$ $(a, b \in \mathbb{R})$ can be obtained as $\varphi(a + bx)$.
- $\ker(\varphi) = (x^2 + 1)$.

Now the above corollary implies that we have

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}\,.$$

Proposition 3.14. *Let $\varphi : R \to S$ be a ring homomorphism. Let $I \subset R$ be an ideal and $\pi : R \to R/I$ the canonical projection.*

If $I \subset \ker(\varphi)$ then there exists a unique map $\overline{\varphi} : R/I \to S$ such that $\overline{\varphi} \circ \pi = \varphi$, and $\overline{\varphi}$ is in fact a ring homomorphism.

We can write this statement effectively with the help of a diagram:

$$\begin{tikzcd} R \arrow[d, "\pi"'] \arrow[dr, "\varphi"] & \\ R/I \arrow[r, dashed, "\overline{\varphi}"'] & S \end{tikzcd}$$

Examples 3.15: 1) $\varphi : \mathbb{Z} \to \mathbb{Z}_n (= \mathbb{Z}/(n)_{\mathbb{Z}})$, $n \geqslant 2$, sending a to $\overline{a}$, is a homomorphism of rings. Its kernel is $\ker(\varphi) = (n)_{\mathbb{Z}} = n\mathbb{Z}$, a principal ideal (a single generator being n or $-n$).

$I \subset (n)$ means that $I = (k)$ with $k \in (n)$, i.e., $n \,|\, k$, i.e., $k = mn$ for some $m \in \mathbb{Z}$.

So assuming $k = mn$ we get the diagram

$$\begin{tikzcd} \mathbb{Z} \arrow[d, "\pi"'] \arrow[dr, "\varphi"] & \\ \mathbb{Z}/(mn) \arrow[r, dashed, "\overline{\varphi}"'] & \mathbb{Z}/(n) \end{tikzcd}$$

2) $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_2$, sending $a + bi \to \overline{a + b}$, is a surjective ring homomorphism, with kernel $\ker(\varphi) = (-1 + i)$.

Note that $(4) \subset \ker(\varphi)$ since $\varphi(4) = \overline{0}$. The proposition gives us a map $\overline{\varphi}$ fitting into the following diagram

$$\begin{tikzcd} \mathbb{Z}[i] \arrow[d, "\pi"'] \arrow[dr, "\varphi"] & \\ \mathbb{Z}[i]/(4) \arrow[r, dashed, "\overline{\varphi}"'] & \mathbb{Z}_2 \end{tikzcd}$$

Example 3.16: (Example 3.15, 2) cont'd) Since φ is surjective, we can apply the First Isomorphism Theorem for rings, giving

$$\mathbb{Z}[i]/(-1 + i) \cong \mathbb{Z}_2\,,$$

where the map is given by $a + bi + (-1 + i)_{\mathbb{Z}[i]} \mapsto \overline{a + b}$.

Operations on ideals: Let R be a ring and I, J ideals in R. Then

1) $I \cap J = \{a \in R \mid a \in I \text{ and } a \in J\}$;
2) $I + J = \{a + b \in R \mid a \in I,\ b \in J\}$;
3) $I \cdot J = \{\sum_{\text{finite}} a_k b_k \in R \mid a_k \in I \text{ and } b_k \in J\}$.

All of the three are ideals, and we have the following inclusions:

$$I \cdot J \subset I \cap J \subset \begin{Bmatrix} I \\ J \end{Bmatrix} \subset I + J \,.$$

Example 3.17: Let $R = \mathbb{Z}$, $I = (4)$={all multiples of 4 inside $\mathbb{Z}$}, $J = (6)$={all multiples of 6 inside $\mathbb{Z}$}. Then $I \cap J$ ={all n in $\mathbb{Z}$ which are multiples of both 4 and 6}, i.e. precisely the multiples of 12, i.e., $I \cap J = (12)$. This example shows in particular that the above inclusions are all strict:

$$(24) \subset (12) \subset \begin{Bmatrix} (4) \\ (6) \end{Bmatrix} \subset (2) \,.$$

Important fact: Let R be a commutative ring with identity. Then we have the following identity of ideals in terms of generators:

$$\begin{aligned} (a_1, \ldots, a_n) + (b_1, \ldots, b_m) &= (a_1, \ldots, a_n, b_1, \ldots, b_m)\,, \\ (a_1, \ldots, a_n) + (b_1, \ldots, b_m) &= (a_1 b_1, \ldots, a_1 b_m, \ldots, a_n b_1, \ldots, a_n b_m)\,. \end{aligned}$$

Example 3.18: In $\mathbb{Z}[\sqrt{-5}]$, we take $I = (2, 3+\sqrt{-5})$, $J = (3, 1-\sqrt{-5})$. Then we have

$$I + J = (2, 3+\sqrt{-5}) + (3, 1-\sqrt{-5}) = (2, 3+\sqrt{-5}, 3, 1-\sqrt{-5}) = (1)\,,$$

since $1 = (-1)\cdot 2 + 1 \cdot 3 + 0 \cdot (3+\sqrt{-5}) + 0 \cdot (1-\sqrt{-5})$.

$$\begin{aligned} \cdot J &= (2, 3+\sqrt{-5}) \cdot (3, 1-\sqrt{-5}) \\ &= \big(2\cdot 3, 2\cdot(1-\sqrt{-5}), (3+\sqrt{-5})\cdot 3, (3+\sqrt{-5})(1-\sqrt{-5})\big) \\ &= \big(6, 2-2\sqrt{-5}, 9+3\sqrt{-5}, 8-2\sqrt{-5}\big) \\ &= \big(6, 2-2\sqrt{-5}, 9+3\sqrt{-5}\big) \qquad [8-2\sqrt{-5} = 6 + (2-2\sqrt{-5})] \\ &= \big(6, 2-2\sqrt{-5}, -3+3\sqrt{-5}\big) \qquad [\text{replace } 9+3\sqrt{-5} = 12 + (-3+3\sqrt{-5}) \text{ by} \\ &\qquad -3+3\sqrt{-5} \text{ since 12 is a linear combination of the other two generators}] \\ &= \big(6, 1-\sqrt{-5})\big) \qquad [\text{replace the last two generators by their gcd}] \\ &= \big(1-\sqrt{-5})\big)\,. \qquad [6 = (1+\sqrt{-5})(1-\sqrt{-5})] \end{aligned}$$

Theorem 3.19. *(Chinese Remainder Theorem for Rings) Let R be a ring and I, $J \subset R$ ideals such that $I + J = R$. Then*

$$\begin{aligned} R/(I \cap J) &\xrightarrow{\cong} R/I \times R/J\,, \\ a &\mapsto (\overline{a}, \overline{a}) = (a+I, a+J)\,. \end{aligned}$$

If R is commutative with identity, then we further have

$$R/(I \cdot J) \xrightarrow{\cong} R/I \times R/J\,,$$

with the same map as above.

Remark 3.20: 1) Suppose R has an identity, then $I + J = R$ if and only if $1 = a + b$ for some $a \in I$, $b \in J$. (I and J are then called **coprime** to each other.)

2) Suppose R is commutative with identity. Then if $I + J = R$, then $I \cap J = I \cdot J$.

Remark 3.21: Suppose R is commutative with identity and I, J ideals in R with $I+J=R$, then we can write $1=a+b$, $a\in I$, $b\in J$.

For $r,s\in R$, we get

$$\begin{aligned} r &= r(a+b) = \overbrace{r\cdot a}^{=:i_r\in I} + \overbrace{r\cdot b}^{=:j_r\in J}\,, \\ s &= s(a+b) = \underbrace{s\cdot a}_{=:i_s\in I} + \underbrace{s\cdot b}_{=:j_s\in J}\,. \end{aligned}$$

Under the above map

$$R/I\cdot J \xrightarrow{\cong} R/I\times R/J$$

we obtain that $sa+rb+I\cdot J$ maps to $(r+I,s+J)$.

Examples 3.22: 1) Let $R=\mathbb{Z}$ and $I=(m)_{\mathbb{Z}}$, $J=(n)_{\mathbb{Z}}$. Then $I+J=\gcd(m,n)$, so $I+J=R\Leftrightarrow \gcd(m,n)=1$.

Suppose that $\gcd(m,n)=1$, so that $I+J=\mathbb{Z}$. Then we have

$$\begin{aligned} \mathbb{Z}/(m\cdot n) &\xrightarrow{\cong} \mathbb{Z}/(m)\times\mathbb{Z}/(n)\,, \\ a+mn\mathbb{Z} &\mapsto (a+m\mathbb{Z},a+n\mathbb{Z})\,. \end{aligned}$$

Make surjectivity explicit: given $b,c\in\mathbb{Z}$, which class in $\mathbb{Z}/(mn)$ maps to $(\overline{b},\overline{c})$?

Write $1=km+\ell n$ for some $k,\ell\in\mathbb{Z}$ (this is possible since $(m,n)=1$). Then we have

$$\begin{aligned} b &= k\cdot m\cdot b+\overbrace{\ell\cdot n\cdot b}^{\in J}\,, \\ c &= \underbrace{k\cdot m\cdot c}_{\in I}+\ell\cdot n\cdot c\,. \end{aligned}$$

Putting these together, we get

$$\overline{\ell nb+kmc}\mapsto(\overline{b},\overline{c})\,.$$

2) $R=\mathbb{Z}[i]$, $I=(2+i)$, $J=(3+i)$. We have $I+J=\mathbb{Z}[i]$ since $1=(-1)\cdot(2+i)+1\cdot(3+i)$.

By the above, $I\cap J=I\cdot J=(2+i)_R\cdot(3+i)_R=\big((2+i)(3+i)\big)_R=(5+5i)_R$, and by the Chinese Remainder Theorem we get

$$\mathbb{Z}[i]/(5+5i)\xrightarrow{\cong}\mathbb{Z}[i]/(2+i)\times\mathbb{Z}[i]/(3+i)\,.$$

We find the element on the left hand side which maps to $(3+I,2+J)$: by the above remark, we take (for $r=3$, $s=2$, $a=-2-i$ and $b=3+i$)

$$(r\cdot b+s\cdot a+I\cdot J=)\quad 3\cdot(3+i)+2\cdot(-2-i)+I\cdot J\,,$$

which can be written slightly simpler as $5+i+I\cdot J$.

Definition 3.23. *Let R be commutative with identity $\mathbb{1}_R\neq 0_R$, and let I be an ideal in R. Then I is called a* **prime ideal** *if*

$$\text{for any } a,b\in R:\big(ab\in I\ \Rightarrow\ a\in I \ \text{ or }\ b\in I\big)\,,$$

and I is called a **maximal ideal** *if*

$$\text{for any ideal } J\subset R \text{ with } I\subset J\subset R \text{ we have either } J=I \text{ or } J=R\,.$$

Examples 3.24: For $R = Z$, all the ideals are of the form (n), $n \in \mathbb{Z}$.

1) (0) is a prime ideal (but it is not maximal: e.g., $(0) \underset{\neq}{\subsetneq} (2) \underset{\neq}{\subsetneq} \mathbb{Z}$).
2) $\mathbb{Z}$ is neither a prime ideal nor a maximal ideal in $\mathbb{Z}$.
3) Consider (n) for $n \geqslant 2$.

   If n is a prime number, then (n) is a prime ideal. In fact, it is even a maximal ideal.

   If n is not a prime number, then (n) is not a prime ideal. It is also not maximal.

Theorem 3.25. *Let R be commutative with identity, $I \subset R$ an ideal. Then*

1) *I is a prime ideal in R $\Leftrightarrow$ R/I is an integral domain.*
2) *I is a maximal ideal in R $\Leftrightarrow$ R/I is a field.*

Corollary 3.26. *A maximal ideal is also a prime ideal.*