# COURSE 7

## Irreducible elements, prime elements

We know that for an integer $p \in \mathbb{Z}^*$, $p \neq \pm 1$, for $p$ to be prime, it must fulfill one of the following two equivalent conditions:

i) $p$ has no other divisors but $\pm 1$ and $\pm p$.

ii) $a, b \in \mathbb{Z}$; $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

We will see that for an arbitrary integral domain $(R, +, \cdot)$, the conditions i) and ii) can define different mathematical objects.

In the following part, we consider an integral domain $(R, +, \cdot)$.

**Definition 1.** An element $p \in R^*$ is an **irreducible element** if it satisfies the following conditions:

1) $p$ is not a unit.

2) $p$ has no non-trivial divisors, i.e.

$$x \in R,\ x \mid p \Rightarrow x \text{ is a unit or } x \sim p.$$

**Remarks 2.** a) An element $p \in R^*$ is irreducible if it fulfills the condition 1) from the above definition and any of the following equivalent conditions:

$2')$ $p = xy \Rightarrow x$ is a unit or $y$ is a unit.

$2'')$ $p = xy \Rightarrow x \sim p$ or $y \sim p$.

$2''')$ $[p]$ is a minimal element in $(R/\sim \setminus \{[1]\}, \leq)$.

b) If $p \in R$ is irreducible then any associate of $p$ is also irreducible.

c) A necessary and sufficient condition for a non-zero non-unit of $R$ to be not irreducible is to non-trivially factorize into two factors.

**Examples 3.** a) The irreducible elements $p$ from $(\mathbb{Z}, +, \cdot)$ are the primes and their opposites.

b) Let $R$ be an integral domanin. A no-zero polynomial $f \in R[X]$ which is not a unit is irreducible if and only if it has no non-trivial factorizations. Thus, the polynomial $f = 2X + 2 \in \mathbb{Z}[X]$ is not irreducible in $\mathbb{Z}[X]$ since 2 and $X + 1$ from its decomposition $f = 2(X + 1)$ are both non-units. But the polynomial $2X + 2$ from $\mathbb{R}[X]$ is irreducible since any degree 1 polynomial with coefficiens in a field is irreducible.

c) If $K$ is a field and $f \in K[X]$ has the degree 2 or 3, then $f$ is irreducible if and only if $f$ has no root in $K$. For the polynomials with the degree at least 4, the lack of roots in $K$ means not necessarily that they are irreducible (e.g. $(X^2 + 1)^2 \in \mathbb{R}[X]$ is not irreducible).

d) A polynomial $f \in \mathbb{C}[X]$ is irreducible in $\mathbb{C}[X]$ if and only if $\deg f = 1$.

e) A polynomial $f \in \mathbb{R}[X]$ is irreducible in $\mathbb{R}[X]$ if and only if $\deg f = 1$ of $f = aX^2 + bX + c$ with $a, b, c \in \mathbb{R}$ and $a \neq 0$, and $\Delta = b^2 - 4ac < 0$.

**Remarks 4.** a) If $d \in \mathbb{Z} \setminus \{1\}$ is a square-free integer and $\delta : \mathbb{Z}[\sqrt{d}\,] \to \mathbb{N}$, $\delta(z) = |z \cdot \overline{z}|$ is the norm map, then, for any $z_1, z_2, z \in \mathbb{Z}[\sqrt{d}\,]$:

i) $z_1 | z_2 \ \Rightarrow\ \delta(z_1) | \delta(z_2)$;

ii) $z_1 \sim z_2 \ \Leftrightarrow\ \delta(z_1) = \delta(z_2)$ and $z_1 | z_2$;

iii) $\delta(z_1) = \delta(z_2)$ does not imply, in general, $z_1 \sim z_2$;

iv) if $\delta(z)$ is a prime then $z$ is an irreducible element of $\mathbb{Z}[\sqrt{d}]$.

b) In the integral domain $(\mathbb{Z}[i], +, \cdot)$ the elements $1+i$ are $1+2i$ are irreducible elements (because of iv) above), 3 and 7 are irreducible elements (even if their norm is not a prime), and 2, 5 and 17 are not irreducible elements.

**Definition 5.** An element $p \in R^*$ is a **prime element** if it saisfies the following conditions:
$\alpha$) $p$ is not a unit.
$\beta$) $x, y \in R;\ p \mid xy \Rightarrow p \mid x$ or $p \mid y$.

**Remarks 6.** a) If $p \in R$ is a prime element, then any associate of $p$ in $R$ is also a prime element.
b) If $p \in R$ is a prime element and $p$ divides the product $x_1 \dots x_n$ of elements of $R$ then $p$ divides at least one of the factors $x_1, \dots, x_n$.

**Examples 7.** i) The prime elements of $(\mathbb{Z}, +, \cdot)$ are the (natural) primes and their opposites.
ii) In the integral domain $(\mathbb{Z}[i\sqrt{5}], +, \cdot)$, $i\sqrt{5}$ is a prime element, 3 is an irreducible element which is not a prime element.

**Theorem 8.** For an integral domanin $R$ we have:
1) Any prime element from $R$ is an irreducible element.
2) If any two elements of $R$ have a gcd, then any irreducible element of $R$ is a prime element.

We proved in the previous course that in a PID $R$, there exists a gcd for any $a, b \in R$ and

$$d = (a, b) \Leftrightarrow dR = aR + bR.$$

Thus, from the previous theorem one deduces the following:

**Corollary 9.** In a PID, an element is irreducible if and only if it is prime.

Since $\mathbb{Z}$ is a PID, the previous corollary gives, once again, a reason why the integers which are prime numbers are the same as the integers which are irreducible numbers. But, as example 7 ii) shows, the converse of the statement 1) from the previous theorem is not always valid.

**Remarks 10.** a) From the statement 2) of the previous theorem and the fact that 3 is irreducible in $\mathbb{Z}[i\sqrt{5}]$, but not prime, we expect to find elements in $\mathbb{Z}[i\sqrt{5}]^*$ which have no gcd. For instance, 6 and $2(1+i\sqrt{5})$ have no gcd in $\mathbb{Z}[i\sqrt{5}]$. Yet, 3 and $1+i\sqrt{5}$ are coprime in $\mathbb{Z}[i\sqrt{5}]$, so they have a gcd (and it is 1).
b) From remark a) one deduces that $\mathbb{Z}[i\sqrt{5}]$ is not a PID. One reason why we did not involve the notion of prime element in the examples we gave in $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Z}[i]$ is that each one of these integral domains is a PID (and even more, as we will further see) so, in these integral domains the notions of prime element and irreducible element coincide.