Definition 22.1

Let R be an integral domain. An element $a \in R$ is *irreducible* if $a \neq 0$, a is not a unit and if $a = bc$ for some $b, c \in R$ then either b or c is a unit.

Example.

- $n \in \mathbb{Z}$ is irreducible and only if $n = \pm p$ where p is a prime number.
- A field has no irreducible elements.
- Take $p(x) \in \mathbb{R}[x]$, $p(x) = x^2 + 1$. Then $p(x)$ is irreducible in $\mathbb{R}[x]$.
- Take $p(x) \in \mathbb{C}[x]$, $p(x) = x^2 + 1$. Then $p(x)$ is not irreducible in $\mathbb{C}[x]$: since $p(x) = (x - i)(x + i)$.

Theorem 22.2

If R is an integral domain, $a \in R$ is irreducible and $u \in R$ is a unit then ua is irreducible.

Proof. Let $ua = bc$. We need to show that either b or c is a unit. Since $a = (u^{-1}b)c$ and a is irreducible, thus either c is a unit or $u^{-1}b$ is a unit. In the second case, since a product of units is a unit, we obtain that $b = u(u^{-1}b)$ is a unit. □

Definition 22.3

Let R be an integral domain. Elements $a, b \in R$ are *associates* if $a = ub$ for some unit $u \in R$. We write: $a \sim b$.

Example.

- If $m, n \in \mathbb{Z}$ then $m \sim n$ iff $m = \pm n$.
- Check: units in $\mathbb{R}[x]$ are non-zero polynomials of degree 0. It follows that if $p(x), q(x) \in \mathbb{R}[x]$ then $p(x) \sim q(x)$ iff $p(x) = aq(x)$ for some $a \in \mathbb{R} - \{0\}$.

Definition 22.4

A *unique factorization domain* (*UFD*) is an integral domain R that satisfies the following conditions:

1) if $a \in R$ is a non-zero, non-unit element then

$$a = b_1 \cdot \ldots \cdot b_k$$

for some irreducible elements $b_1, \ldots, b_k \in R$

2) if $b_1, \ldots, b_k$, $c_1, \ldots, c_l$ are irreducible elements such that

$$b_1 \cdot \ldots \cdot b_k = c_1 \cdot \ldots \cdot c_l$$

then $k = l$ and for some permutation $\sigma\colon \{1, \ldots, k\} \to \{1, \ldots, k\}$ we have $b_1 \sim c_{\sigma(1)}$, $\ldots$, $b_k \sim c_{\sigma(k)}$.

Example.

- $\mathbb{Z}$ is a UFD by the Fundamental Theorem of Arithmetic.
- If F is a field then F is a UFD since all non-zero elements of F are units.

Note. For an positive integer K let $\mathbb{Z}[\sqrt{-K}]$ denote the ring defined as follow:

- Elements of $\mathbb{Z}[\sqrt{-K}]$ are expressions $a + b\sqrt{K}i$ for $a, b \in \mathbb{Z}$.
- Addition:
$$(a + b\sqrt{n}i) + (c + d\sqrt{K}i) = (a + c) + (b + d)\sqrt{K}i$$
- Multiplication:
$$(a + b\sqrt{K}i) \cdot (c + d\sqrt{K}i) = (ac - Kbd) + (ad + bc)\sqrt{K}i$$

The ring $\mathbb{Z}[\sqrt{-K}]$ is a subring of the field of complex numbers $\mathbb{C}$, so it is an integral domain.

Theorem 22.5

The ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Proof. For $a + b\sqrt{5}i \in \mathbb{Z}[\sqrt{-5}]$ define

$$N(a + b\sqrt{5}i) = (a + b\sqrt{5}i)(a - b\sqrt{5}i) = a^2 + 5b^2 \in \mathbb{N}$$

Notice that for any $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ we have:

1) $N(\alpha) = 1$ iff $\alpha = \pm 1$

2) $N(\alpha) = 0$ iff $\alpha = 0$

3) $N(\alpha\beta) = N(\alpha)N(\beta)$

4) $N(\alpha) \neq 3$ for all $\alpha \in \mathbb{Z}[\sqrt{-5}]$

Observation 1. The only units in $\mathbb{Z}[\sqrt{-5}]$ are 1 and -1.

Indeed, if $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is a unit then

$$N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$$

Therefore $N(\alpha) = 1$, and so $\alpha = \pm 1$.

As a consequence we obtain that in $\mathbb{Z}[\sqrt{-5}]$ we have $\alpha \sim \beta$ if and only of $\alpha = \pm\beta$.

Observation 2. If $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is an element such that $N(\alpha) = 9$ then α is irreducible.

Indeed, if $\alpha = \beta\beta'$ then

$$N(\beta)N(\beta') = N(\alpha) = 9$$

Therefore $N(\beta)$ must be either 1 (and so β is a unit), 3 (impossible), or 9 (and then $N(\beta') = 1$, i.e. β' is a unit) .

Take $9 \in \mathbb{Z}[\sqrt{-5}]$. We have

$$3 \cdot 3 = 9 = (2 + \sqrt{5}i)(2 - \sqrt{5}i)$$

By Observation 2 the elements 3, $2 + \sqrt{5}i$, $2 - \sqrt{5}i$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. On the other hand, by Observation 1 we obtain

$$3 \not\sim (2 + \sqrt{5}i), \quad 3 \not\sim (2 - \sqrt{5}i)$$

As a consequence 9 does not have a unique factorization in $\mathbb{Z}[\sqrt{-5}]$. □