0.1. Prerequisites

- $I \subset R$ is an ideal if $\forall (a, b) \in \mathbb{R}^2, ab \in I \Longrightarrow a \in I \vee b \in I$.
- I is maximal if $I \neq R$ and there is no ideal $J \subset R$ such that $I \subset J$.
- $p \in \mathbb{Z}$ is prime iff $\langle p \rangle = \langle p \rangle_{\mathbb{Z}}$ is a prime ideal.
- For commutative ring R:
  - $I \subset R$ is prime ideal iff R/I is an integral domain.
  - I is maximal iff R/I is a field.
- Let R be PID and $a \in R$ irreducible. Then $\langle a \rangle = \langle a \rangle_R$ is maximal.
- **Theorem**: let F be field, $f(x) \in F[x]$ irreducible. Then $F[x]/\langle f(x) \rangle$ is a field and a vector space over F with basis $B = \left\{1, \overline{x}, ..., \overline{x}^{n-1}\right\}$ where $n = \deg(f)$. That is, every element in $F[x]/\langle f(x) \rangle$ can be uniquely written as a linear combination

$$a_0 + a_1\overline{x} + \cdots + a_{n-1}\overline{x}^{n-1}$$

1. Divisibility in rings

1.1. Every ED is a PID

- **Definition**: let R integral domain. $\varphi : R - \{0\} \to \mathbb{N}_0$ is **Euclidean function (norm)** on R if:
  - $\forall x, y \in R - \{0\}, \varphi(x) \leq \varphi(xy)$.
  - $\forall x \in R, y \in R - \{0\}, \exists q, r \in R : x = qy + r$ with either $r = 0$ or $\varphi(r) < \varphi(y)$.
- R is **Euclidan domain (ED)** if a Euclidean function is defined on it.
- Examples of EDs:
  - $\mathbb{Z}$ with $\varphi(n) = |n|$.
  - $F[x]$ for field F with $\varphi(f) = \deg(f)$.
- **Lemma**: $\mathbb{Z}\left[-\sqrt{2}\right]$ is an ED with Euclidean function with

$$\varphi\left(a + b\sqrt{-2}\right) = N\left(a + b\sqrt{-2}\right) =: a^2 + 2b^2.$$

- **Proposition**: every ED is a PID.

1.2. Every PID is a UFD

- **Definition**: Integral domain R is **unique factorisation domain (UFD)** if every non-zero non-unit in R can be written uniquely (up to order of factors and multiplication by units) as product of irreducible elements in R.
- **Example**: let $R = \{f(x) \in \mathbb{Q}[x] : f(0) \in \mathbb{Z}\}$. Its units are ± 1. Any factorisation of $x \in R$ must be of the form $f(x)g(x)$ where $\deg f = 1, \deg g = 0$, so $x = (ax + b)c$, $a \in \mathbb{Q}$, $b, c \in \mathbb{Z}$. We have $bc = 0$ and $ac = 1$ hence $x = \frac{x}{c} \cdot c$. So x irreducible if $c \neq \pm 1$. Also, any factorisation of $\frac{x}{c}$ in R is of the form $\frac{x}{c} = \frac{x}{cd} \cdot d$, $d \in \mathbb{Z}$, $d \neq 0$. Again, neither factor is a unit when $d \neq \pm 1$. So $x = \frac{x}{c} \cdot c = \frac{x}{cd} \cdot c \cdot c = \cdots$ can never be decomposed into irreducibles (the first factor is never irreducible).
- **Lemma**: let R be PID. Then every irreducible element is prime in R.
- **Theorem**: every PID is a UFD.