1. Rings, subrings and fields

- **Ring R**: set with binary operations addition and subtraction, where $(R, +)$ is an abelian group and:
  - **Identity**: exists $1 \in R$ such that $\forall x \in R, 1 \cdot x = x \cdot 1 = x$
  - **Associativity**: for every $x, y, z \in R, x(yz) = (xy)z$
  - **Distributivity**: for every $x, y, z \in R, x(y + z) = xy + xz$ and $(y + z)x = yx + zx$
- **Set of remainders modulo n (residue classes)**: $\mathbb{Z} / n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$
- $\mathbb{Z} / n$ is a ring: $\overline{a} + \overline{b} = \overline{a+b}, \overline{a} - \overline{b} = \overline{a-b}, \overline{a} \cdot \overline{b} = \overline{a \cdot b}$
- **Subring S** of ring R: a set $S \subseteq R$ that contains 0 and 1 and is closed under addition, multiplication and negation:
  - $0 \in S, 1 \in S$
  - $\forall a, b \in S, a + b \in S$
  - $\forall a, b \in S, ab \in S$
  - $\forall a \in S, -a \in S$
- **Field F** is a ring with:
  - F is commutative
  - $0 \neq 1 \in F$ (F has at least two elements)
  - $\forall 0 \neq a \in R, \exists b \in R, ab = 1$. b is the **inverse** of a
- a is a **zero divisor** if $ab = 0$ for some $b \neq 0$

2. Integral domains

- **Integral domain R**: ring which is commutative, has at least two elements ($0 \neq 1$), and has no zero divisors apart from 0
- Any subring of a field is an integral domain
- If R is an integral domain, then $R[x] = \{a_0 + a_1x + ... + a_nx^n : a_i \in R\}$ is also an integral domain.
- a is a **unit** if $ab = ba = 1$ for some $b \in R$. $b = a^{-1}$ is the **inverse** of a
- Inverses are unique
- $R^\times$, set of all units in R, is a group under multiplication of R
- For field F, $F^\times = F - \{0\}$
- $a \in \mathbb{Z} / n$ is a unit iff $\gcd(a, n) = 1$
- $\mathbb{Z} / p$ is a field iff p is prime
- $\mathbb{Z} / n$ is an integral domain iff n is prime (iff $\mathbb{Z} / n$ is a field)

3. Polynomials over a field

- **Degree** of $f(x) = a_0 + a_1x + ... + a_nx^n$:

$$\deg(f) = \begin{cases} \max\{i : a_i \neq 0\} & \text{if } f \neq 0 \\ -\infty & \text{if } f = 0 \end{cases}$$

- $\deg(fg) = \deg(f) + \deg(g)$
- $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
- If $\deg(f) \neq \deg(g)$ then $\deg(f + g) = \max\{\deg(f), \deg(g)\}$

- Let $f(x), g(x) \in F[x]$, $g(x) \neq 0$, then $\exists q(x), r(x) \in F[x]$ with $\deg(r) < \deg(g)$ such that $f(x) = q(x)g(x) + r(x)$

4. Divisibility and greatest common divisor in a ring

- a **divides** b, $a \mid b$, if $\exists r \in R$ such that $b = ra$
- d is a **greatest common divisor** of a and b, $\gcd(a, b)$, if:
  - $d \mid a$ and $d \mid b$ and
  - If $e \mid a$ and $e \mid b$ then $e \mid d$
- $\gcd(0, 0) = 0$
- **Euclidean algorithm example**: find gcd of $f(x) = x^2 + 7x + 6$ and $g(x) = x^2 - 5x - 6$ in $\mathbb{Q}[x]$:

$$\begin{aligned} f(x) &= g(x) + 12(x+1) \\ g(x) &= \frac{1}{12}x \cdot 12(x+1) - 6(x+1) \\ 12(x+1) &= -2 \cdot -6(x+1) + 0 \end{aligned}$$

  Remainder is now zero so stop. A gcd is given by the last non-zero remainder, $-6(x+1)$. We can write $-6(x+1)$ as a combination of $f(x)$ and $g(x)$:

$$\begin{aligned} -6(x+1) &= g(x) - \frac{1}{12}x \cdot 12(x+1) \\ &= g(x) - \frac{1}{12}x \cdot (f(x) - g(x)) \\ &= \left(1 + \frac{1}{12}x\right)g(x) - \frac{1}{12}xf(x) \end{aligned}$$

- Let R be integral domain, $a, b \in R$ and $d = \gcd(a, b)$. Then $\forall u \in R^\times$, ud is also a $\gcd(a, b)$. Also, for d and d' gcds of a and b, $\exists u \in R^\times$ such that $d = ud'$ (so gcd is unique up to units).
- Polynomial is **monic** if leading coefficient is 1
- There always exists a unique monic gcd of two polynomials in $F[x]$
- Let $R = \mathbb{Z}$ or $F[x]$, $a, b \in R$. Then
  - A $\gcd(a, b)$ always exists
  - $a \neq 0$ or $b \neq 0$ then a $\gcd(a, b)$ can be computed by Euclidean algorithm
  - If d is a $\gcd(a, b)$ then $\exists x, y \in R$ such that $ax + by = d$

5. Factorisations in rings

- $r \in R$ **irreducible** if:
  - $r \notin R^\times$ and
  - If $r = ab$ then $a \in R^\times$ or $b \in R^\times$
- $a \in F$ is **root** of $f(x) \in F[x]$ if $f(a) = 0$
- Let $f(x) \in F[x]$.
  - If $\deg(f) = 1$, f is irreducible.
  - If $\deg(f) = 2$ or 3 then f is irreducible iff it has no roots in F.

    - If $\deg(f) = 4$ then f is irreducible iff it has no roots in F and it is not the product of two quadratic polynomials.
- Let $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[x]$, $\deg(f) \geq 1$. If $f(p / q) = 0$, $\gcd(p, q) = 1$, then $p \mid a_0$ and $q \mid a_n$.
- **Gauss's lemma**: let $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[x]$, $\deg(f) \geq 1$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ iff it is irreducible in $\mathbb{Q}[x]$ and $\gcd(a_0, a_1, ..., a_n) = 1$.
- If monic polynomial in $\mathbb{Z}[x]$ factors in $\mathbb{Q}[x]$ then it factors into integer monic polynomials.
- Let R be commutative, $x \in R$ be irreducible and $u \in R^\times$. Then ux is also irreducible.
- **Eisenstein's criterion**: let $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[x]$, p be prime with $p \mid a_0$, $p \mid a_1, ..., p \mid a_{n-1}$, $p \nmid a_n$, $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$
- Let $f(x) \in F[x]$, then f can be uniquely factorised into a product of irreducible elements, up to order of factors and multiplication by units.
- Let R be commutative. $x \in R$ is **prime** if:
    - $x \neq 0$ and $x \notin R^\times$ and
    - If $x \mid ab$ then $x \mid a$ or $x \mid b$
- If $R = \mathbb{Z}$ or $F[x]$ then $a \in R$ is prime iff it is irreducible.
- Let R be an integral domain and $x \in R$ prime. Then x is irreducible.
- Integral domain R is **unique factorisation domain (UFD)** if every non-zero non-unit element in R can be written as a unique product of irreducible elements, up to order of factors and multiplication by units.

6. Ring homomorphisms

- For R, S rings, $f : R \to S$ is **homomorphism** if:
    - $f(1) = 1$ and
    - $f(a + b) = f(a) + f(b)$ and
    - $f(ab) = f(a) f(b)$
- Let $f : R \to S$ homomorphism, then
    - $f(0) = 0$ and
    - $f(-a) = f(a)$
- **Kernel**:

$$\ker(f) := \{a \in R : f(a) = 0\}$$

- **Image**:

$$\operatorname{Im}(f) := \{f(a) : a \in R\}$$

- **Isomorphism**: bijective homomorphism.
- R and S **isomorphic**, $R \cong S$ if there exists isomorphism between them.
- Homomorphism f injective iff $\ker(f) = \{0\}$.
- **Direct product** of R and S, $R \times S$:
    - $(r, s) + (r', s') = (r + r', s + s')$.
    - $(r, s)(r', s') = (rr', ss')$.
    - Identity is $(1, 1)$.

- For $p_1(r,s) = r$ and $p_2(r,s) = s$, $\ker(p_1) = \{(0,s) : s \in S\}$ and $\ker(p_2) = \{(r,0) : r \in R\}$. These are both rings, with $\ker(p_1) \cong S$ (via $(0,s) \to s$) and $\ker(p_2) \cong R$ (via $(r,0) \to r$). ($\ker(p_1)$ and $\ker(p_2)$ are not subrings of $R \times S$ though). So

$$\ker(p_1) \times \ker(p_2) \cong R \times S$$

7. Ideals and quotient rings

- $I \subseteq R$ is an **ideal** if I closed under addition and if $x \in I$, $r \in R$ then $rx \in I$ and $xr \in I$.
- **Left ideal**: I closed under addition and if $x \in I$, $r \in R$ then $rx \in I$.
- **Right ideal**: I closed under addition and if $x \in I$, $r \in R$ then $xr \in I$.
- If $x \in I$, then $(-1)x = x(-1) = -x \in I$ so I closed under negation.
- For $f : R \to S$ homomorphism, $\ker(f)$ is ideal of R.
- For R commutative ring and $a \in R$, **principal ideal generated by a** is

$$(a) := \{ra : r \in R\}$$

- For R commutative and $a_1, ...a_n \in R$,

$$(a_1, ..., a_n) := \{r_1 a_1 + \cdots + r_n a_n : r_1, ..., r_n \in R\}$$

  is an ideal. $(a_1, ..., a_n)$ is **generated** by $a_1, ..., a_n$. $a_i \in (a_1, ..., a_n)$ for all i.
- If ideal I contains unit u, then $u^{-1}u = 1 \in I$ so $\forall r \in R, r \cdot 1 = r \in I$. So $R \subseteq I$ so $R = I$.
- For field F, any ideal is either $\{0\}$ or F.
- Let $I_1 = (a_1, ..., a_m)$, $I_2 = (b_1, ..., b_n)$ then $I_1 = I_2$ iff $a_1, ..., a_m \in I_2$ and $b_1, ..., b_n \in I_1$.
- $a, b \in R$ **equivalent modulo I** if $a - b \in I$. Write $\overline{a} = \overline{b}$ or $a \equiv b \pmod{I}$.
- Let $a(x) \in \mathbb{Q}[x]$, then $p(x) = q(x)a(x) + r(x)$ with $\deg(r) < \deg(a)$. $p(x) - r(x) = q(x)a(x) \in (a(x))$ so $\overline{p(x)} = \overline{r(x)}$. $r(x)$ is **representative** of the class $\overline{p(x)}$.
- Let $I \subseteq R$ ideal. **Coset** of I generated by $x \in I$ is

$$\overline{x} := x + I = \{x + r : r \in I\} \subseteq R$$

  x is a **representative** of $x + I$.
- For $x, y \in R$,

$$x + I = y + I \Longleftrightarrow x + I \cap y + I \neq \emptyset \Longleftrightarrow x - y \in I$$

- If x is a representative of $x + I$, so is $x + r$ for every $r \in I$.
- **Quotient** of R by I ("$R \bmod I$"): set of all cosets of R by I:

$$R / I := \{\overline{x} : x \in R\} = \{x + I : x \in R\}$$

  with
  - $(x + I) + (y + I) = (x + y) + I$.
  - $(x + I)(y + I) = xy + I$.
- R / I is a ring, with zero element $0 + I = I$ and identity $1 + I \in R / I$.
- **Quotient map (canonical map/homomorphism)**: $R \to R / I, r \to \overline{r} = r + I$.
- Kernel of quotient map is I and image is R / I. Hence every ideal is a kernel.

- **First isomorphism theorem (FIT)**: Let $\varphi : R \to S$ be homomorphism. Then

$$\overline{\varphi} : R \,/\, \ker(\varphi) \to \operatorname{Im}(\varphi), \overline{\varphi}(\overline{x}) = \varphi(x)$$

  is an isomorphism: $R \,/\, \ker(\varphi) \cong \operatorname{Im}(\varphi)$.

8. Prime and maximal ideals

- Ideal $I \subseteq R$ **prime ideal** if $I \neq R$ and $ab \in I \Longrightarrow a \in I$ or $b \in I$.
- $I \subseteq R$ **maximal** if only ideals containing I are I and R (so no ideals strictly between I and R).
- $x \in R$ is prime iff (x) is prime ideal.
- To contain is to divide:

$$a \in (x) \Longleftrightarrow (a) \subseteq (x) \Longleftrightarrow x \mid a$$

- For R commutative and I ideal:
  - I prime iff $R \,/\, I$ integral domain.
  - I maximal iff $R \,/\, I$ field.
- (I, x) is ideal generated by I and x:

$$(I, x) : \{rx + x' : r \in R, x' \in I\}$$

- If I is maximal ideal, then it is prime.

9. Principal ideal domains

- **Principal ideal domain (PID)**: integral domain where every ideal is principal.
- $\mathbb{Z}$, $F[x]$, $\mathbb{Z}[i]$ and $\mathbb{Z}\left[\sqrt{\pm 2}\right]$ are PIDs.
- Every PID is a UFD.
- Let R be PID and $a, b \in R$. Then $d = \gcd(a, b)$ exists and $(d) = (a, b)$.

10. Fields as quotients

- Let R be PID, $a \in R$ irreducible. Then (a) is maximal.
- Let $f(x) \in F[x]$ irreducible. Then $F[x] \,/\, (f(x))$ is field and $F[x] \,/\, (f(x))$ is a vector space over F with basis $\left\{\overline{1}, \overline{x}, ..., \overline{x}^{n-1}\right\}$ where $n = \deg(f)$. So every element in $F[x] \,/\, f(x)$ can be uniquely written as $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$, $a_i \in F$.
- Let p prime and $n \in \mathbb{N}$, then there exists irreducible $f(x) \in (\mathbb{Z} \,/\, p)[x]$ with $\deg(f) = n$ and $(\mathbb{Z} \,/\, p)[x] \,/\, (f(x))$ is a field with p^n elements. Any two such fields are isomorphic so unique (up to isomorphism) field with p^n elements is written $\mathbb{F}_{p^n}$.

11. The Chinese remainder theorem

- $a, b \in R$ **coprime** if no irreducible element divides a and b.
- Let R be PID, $a, b \in R$ coprime. Then $(a, b) = (1) = R$ so $ax + by = 1$ for some $x, y \in R$. So any $\gcd(a, b)$ is a unit.
- **Chinese remainder theorem (CRT)**: Let R be PID, $a_1, ..., a_k$ pairwise coprime. Then

$$\varphi : R \,/\, (a_1 \cdots a_k) \to R \,/\, (a_1) \times \cdots \times R \,/\, (a_k)$$
$$\varphi(r + (a_1 \cdots a_k)) = (r + (a_1), ..., r + (a_k))$$

is an isomorphism.