Definitions you should know

Ring: A set with addition, subtraction, and multiplication subject to the usual rules

Integral domain: a ring without zero divisors, i.e.

\[ ab = 0 \implies a = 0 \text{ or } b = 0 \]

\[ \mathbb{Z} \text{ integers} \]

Field: Commutative ring in which each nonzero element has an inverse.
Ideal: a subgroup $I$ of a ring $R$ with $a x \in I$ for any $a \in R$ and $x \in I$.

Prime ideal: if $a b \in I$ then $a \in I$ or $b \in I$.

Principal ideal: generated by a single element.

E.g.: $(3, x) \subset \mathbb{Z}[x]$ is not principal.

Maximal ideal: the only bigger ideal is $(1) = R$. 

Principal ideal domain (PID)

An integral domain in which every ideal is principal.

e.g. \( \mathbb{Z} \) is a PID

Constructions

Given a ring \( R \) and an ideal \( I \subset R \)

\( R/I \) is the quotient ring.

\( I \) is prime \( \iff \) \( R/I \) is a domain

\( I \) is maximal \( \iff \) \( R/I \) is a field

\( \text{e.g. } \mathbb{Z}/(5) = \text{field} \)
A ring homomorphism \( \phi : R \rightarrow S \) is a map preserving addition and multiplication:

\[
\begin{align*}
\phi(a + b) &= \phi(a) + \phi(b) \\
\phi(a - b) &= \phi(a) - \phi(b) \\
\phi(ab) &= \phi(a) \phi(b)
\end{align*}
\]

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

\( \ker \phi \) is an ideal and image of \( \phi \) is isomorphic to \( R / \ker \phi \).
Given a domain $D$ one constructs its field $F$ of quotients as follows:

\[ \mathbb{Z} \longrightarrow \mathbb{Q} \]

$F$ consists of "fractions" all

where $a, b \in D$ with $b \neq 0$

\[ \frac{a}{b} = \frac{c}{d} \quad \text{if} \quad ad = bc \]

\[ \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \]

\[ \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \]
$R[x] = \text{ring of polynomials in } x \text{ over a ring } R$

$= \{ m_0 + m_1 x + \cdots + m_n x^n : m_i \in R \}$

Properties of $F[x]$ for a field $F$

Division algorithm: Given $f(x), g(x) \in F[x]$ with $g(x) \neq 0$

$\exists! q(x) \text{ and } r(x)$ so that

$f(x) = q(x)g(x) + r(x)$

with $\deg r(x) < \deg g(x)$
The greatest common divisor of \( f(x) \) and \( g(x) \) is (up to nonzero constant multiplication) the polynomial dividing both \( f \) and \( g \) with largest possible degree.

\[ \begin{align*}
\text{e.g.} \quad f &= (x+1)^3 \\
g &= (x+1)^2(x+2) \\
gcd(f, g) &= (x+1)^2 
\end{align*} \]

Euclidean algorithm to find \( \gcd(f, g) \):

Assume \( \deg g \leq \deg f \).
Use division to write (let $g = m_0$)

\[ f = g_1 \cdot g + m_1 \]

If $m_1 = 0$, $g = \text{gcd}$

If $m_1 \neq 0$, then divide $g$ by $m_1$,

\[ g = g_2 \cdot m_1 + m_2 \]

If $m_2 = 0$, then $m_1 = \text{gcd}$

If $m_2 \neq 0$, divide $m_1$ by $m_2$

\[ m_1 = g_3 \cdot m_2 + m_3 \]

\[ \deg(g) > \deg(m_1) > \deg(m_2) > \cdots \]

After a finite \# of steps we get remainder 0. The $\text{gcd}$ is the last nonzero remainder.
Applications of Division Algorithm

Factor theorem

\[ f(a) = 0 \quad \text{for} \quad a \in F \Leftrightarrow \]
\[ f(x) = (x-a) \cdot g(x) \]

\(a\) is a zero of \(f\).

Let \( \deg f = n \). Then \( f(x) \) has at most \( n \) zeroes.

Theorem 6.3.12 For a finite field \( F \), the group \( F^* = \{ a \in F : a \neq 0 \} \) under multiplication is cyclic.
A polynomial $f(x) \in F[x]$ is irreducible if it cannot be factored, i.e., it is not the product of two polynomials of smaller degree.

Thm 3.4.6. Factorization of polynomials is unique. Any polynomial is a product of irreducible ones.
Two tests for irreducibility in $\mathbb{Z}[x]$

1) Eisenstein criterion

A monic polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

is irreducible if

i) $p | a_i$ for $1 \leq i \leq n$

ii) $p^2 \nmid a_n$

2) Given $f(x) \in \mathbb{Z}[x]$, look at its image $\bar{f}$ in $\mathbb{Z}/p[\mathbb{Z}]$. If $\bar{f}$ is irreducible, so is $f$. 
Notation: Book uses \( \langle f(x) \rangle \) to denote the ideal generated by \( f(x) \). Everyone else denotes it by \( (f(x)) \).

**Theorem:** \( \mathbb{F}[x]/\langle f(x) \rangle \) or \( \mathbb{F}[x]/(f(x)) \) is a field \( \iff \) \( f(x) \) is irreducible.

**Given:** \( \mathbb{F} \subset \mathbb{E} \) fields with \( x \in \mathbb{E} \).

**Then:** \( \mathbb{F}[x] \) - all expressions of the form \( f(x) \) for \( f(x) \in \mathbb{F}[x] \).

\( = \) subring of \( \mathbb{E} \).
$F(\alpha) = \text{all expressions } \frac{f(\alpha)}{g(\alpha)}$ where $f, g \in F[x]$ with $g \neq 0$.

$E = \text{subfield of } F(\alpha)$ is the extension of $F$ obtained by adjoining $\alpha$.

$F = \mathbb{Q}, E = \mathbb{C}, \alpha = \pi$ but $\pi$ is transcendental.

$F[\alpha] \ni 7 + \pi - 53\pi^2 + \frac{\pi^3}{36}$ but not $\frac{1}{\pi}$.

$F(\alpha) \ni \frac{1}{\pi}, \frac{2}{3 + \pi^2}$ but not a field.

$\alpha = \sqrt{2}$, then $\mathbb{Q}[\sqrt{2}]$ is a field.
\[
\frac{1}{a - k \sqrt{2}} = \frac{a + k \sqrt{2}}{(a + k \sqrt{2})(a - k \sqrt{2})} = \frac{a - k \sqrt{2}}{a^2 - 2k^2}
\]

\( \mathbb{Q}(\sqrt{2}) \) is a field. \( \sqrt{2} \) is algebraic.

Thm 10.2.5 (Kronecker) Given a nonconstant \( p(x) \in \mathbb{F}[x] \), there is a field \( E \supseteq \mathbb{F} \) and \( \alpha \in E \) with \( p(\alpha) = 0 \).

Given \( \mathbb{F} \subseteq E \) and \( \alpha \in E \), \( \alpha \) is algebraic over \( \mathbb{F} \) if there is a nonzero polynomial \( p(x) \in \mathbb{F}[x] \) with \( p(\alpha) = 0 \).
otherwise $\alpha$ is transcendental

If $\alpha$ is algebraic, its minimal polynomial $p(x)$ is the monic polynomial of least degree with $p(\alpha) = 0$.

e.g. $\alpha = \sqrt[3]{3} + \sqrt{2}$, $F = \mathbb{Q}$, $E = \mathbb{R}$

$\alpha^2 = 3 + 2\sqrt{6} + 2 = 5 + 2\sqrt{6}$

$\alpha^2 \frac{5}{2} = 2\sqrt{6}$

$(\alpha^2 - 5)^2 = 24$

$= \alpha^4 - 10\alpha^2 + 25$

$\alpha^4 - 10\alpha^2 + 1 = 0$
Theorem 10.2.11: Let \( p(x) \in \mathbb{F}[x] \) be the minimal polynomial of \( \alpha \in E \supseteq \mathbb{F} \). Then
\[
E(\alpha) = \mathbb{F}[x]/(p(x))
\]
e.g. \( \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}[x]/(x^4 - 10x^2 + 1) \)

An extension as above is algebraic, i.e. \( \mathbb{F}(\alpha) \) is an algebraic extension of \( \mathbb{F} \).

A field extension \( E \mid \mathbb{F} \) is finite if \( E \) is a finite dimensional
vector space \( \mathbf{V} \), degree \( [E:F] \) in this dimension

\( F \rightarrow E \rightarrow K \) finite extensions

then \( [K:F] = [K:E][E:F] \)