Proposition 1. Let $(R,+,\cdot)$ be a ring.

(a) $-0=0$ and $-(-x)=x$ for every $x\in R$.

(b) If $x,y,z\in R$ then $x+z=y+z \implies x=y$ and $z+x=z+y \implies x=y$.

(c) If $n\in\mathbb{Z}$ and $x\in R$, define

$$nx=\begin{cases} x+\cdots+x \quad (n \text{ times}) & \text{if } n>0,\\ 0 & \text{if } n=0,\\ -x-\cdots-x \quad (-n \text{ times}) & \text{if } n<0. \end{cases}$$

Then $(n+m)x=nx+mx$ and $n(mx)=(nm)x$ for all $n,m\in\mathbb{Z}$ and $x\in R$.

Proposition 2. If R is a ring, then $0_R\cdot x=0_R$ and $x\cdot 0_R=0_R$ for all $x\in R$.

Proposition 3. (a) If R is a unital ring and $x\in R$ is invertible, then x is not a zero-divisor.

(b) If R is a division ring, then R contains no zero-divisors.

Lemma 4. If R is a unital ring and $a,x,b\in R$ with $ax=1_R$ and $xb=1_R$, then x is invertible and $a=b=x^{-1}$.

Lemma 5. If R is a ring with no zero-divisors, then

$$xy=0 \implies x=0 \text{ or } y=0$$

for all $x,y\in R$.

Proposition 6 (Cancellation in a ring with no zero-divisors)**.** If R is a ring with no zero-divisors and $x\in R^\times$, then for any $a,x,b\in R$,

(a) $ax=bx \implies a=b$, and

(b) $xa=xb \implies a=b$.

Theorem 7. If R is a finite unital ring with no zero-divisors, then R is a division ring.

Corollary 8. (a) If R is a finite unital ring, then R is a division ring if and only if R has no zero-divisors.

(b) If R is a finite commutative unital ring, then R is a field if and only if R has no zero-divisors.

Lemma 9. If $n \in \mathbb{N}$ with $n > 1$, then n is prime if and only if

$$\forall k, \ell \in \mathbb{Z}, \quad n \mid k\ell \implies n \mid k \text{ or } n \mid \ell.$$

Corollary 10. The ring $(\mathbb{Z}_n, \oplus, \odot)$ is a field if and only if n is prime.

Theorem 11. If $(R, +, \cdot)$ is a ring and $S \subseteq R$, then the following are equivalent:

(a) S is a subring of R;

(b) $(S, +)$ is a subgroup of $(R, +)$ and S is closed under multiplication;

(c) $S \neq \emptyset$, and for all $x, y \in S$ we have $x - y \in S$ and $xy \in S$.

Proposition 12. Let R and S be rings, and let $\theta\colon R \to S$ be a (ring) homomorphism.

(a) $\theta(0_R) = 0_S$

(b) $\theta(-x) = -\theta(x)$ for all $x \in R$

(c) $\theta(x - y) = \theta(x) - \theta(y)$ for all $x, y \in R$

(d) $\theta(mx) = m\theta(x)$ for all $m \in \mathbb{Z}$ and $x \in R$

Proposition 13. Let R and S be rings, and let $\theta\colon R \to S$ be a (ring) homomorphism. The image of θ, that is, the set

$$\theta(R) = \{\theta(x)\colon x \in R\}$$

is a subring of S.

Proposition 14. Let R and S are rings, and let $\theta\colon R \to S$ be a (ring) homomorphism.

(a) If R is a unital ring, then so is $\theta(R)$.

(b) If R is a commutative ring, then so is $\theta(R)$.

(c) θ is injective if and only if $\ker\theta = \{0_R\}$.

Proposition 15. If R and S are rings and $\theta\colon R \to S$ is a (ring) homomorphism, then $\ker\theta$ is an ideal in R.

Theorem/Definition 16. If I is an ideal of a ring R, then there are two well-defined operations on set $R/I = \{I + x\colon x \in R\}$ given by

$$(I + x) + (I + y) = I + (x + y) \quad \text{and} \quad (I + x)(I + y) = I + xy$$

which turn R/I into a ring, called the *quotient ring* of R by I.

Theorem 17 (The first isomorphism theorem; or the fundamental homomorphism theorem for rings)**.** If R and S are rings and $\theta\colon R \to S$ is a homomorphism, then

(a) $\theta(R)$ is a subring of S

(b) $\ker\theta$ is an ideal of R

(c) $R/\ker\theta \approx \theta(R)$.

In fact, if $K = \ker\theta$ then the map $\phi\colon R/K \to \theta(R)$, $K + x \mapsto \theta(x)$ is a well-defined isomorphism.

Corollary 18. If R and S are rings and $\theta\colon R \to S$ is a surjective homomorphism, $R/\ker\theta \approx S$.

Proposition/Definition 19. If $I \lhd R$ then the map $\eta_I\colon R \to R/I$ defined by $\eta_I(x) = I + x$ for $x \in R$ is a surjective homomorphism with kernel I. It is called the *natural homomorphism* $R \to R/I$.

Corollary 20. Let R be a ring.

(a) If $S \subseteq R$, then S is a subring of R if and only if there is a ring T and a homomorphism $\theta\colon T \to R$ so that S is the image of θ.

(b) If $I \subseteq R$, then I is an ideal of R if and only if there is a ring W and a homomorphism $\phi\colon R \to W$ so that $I = \ker\phi$.

Theorem 21 (The second isomorphism theorem)**.** Let R be a ring, let S be a subring of R and let I be an ideal of R. Then

(a) the set $S + I = \{s + i\colon s \in S,\ i \in I\}$ is a subring of R which contains I, and $I \lhd S + I$;

(b) $S \cap I \lhd S$; and

(c) $(S + I)/I \approx S/(S \cap I)$

Theorem 22 (The third isomorphism theorem)**.** Let R be a ring and let I and J be ideals of R with $I \subseteq J$. Then

(a) $I \lhd J$;

(b) $J/I \lhd R/I$; and

(c) $(R/I)/(J/I) \approx R/J$.

Theorem 23 (The correspondence theorem)**.**
If I is an ideal of a ring R, then the maps

$$\alpha\colon \{\text{subrings } S \text{ of } R \text{ with } I \subseteq S\} \to \{\text{all subrings of } R/I\}, \quad \alpha(S) = S/I$$

and

$$\widetilde{\alpha}\colon \{\text{ideals } J \text{ of } R \text{ with } I \subseteq J\} \to \{\text{all ideals of } R/I\}, \quad \widetilde{\alpha}(J) = J/I$$

are both well-defined bijections.

Proposition 24. Let R be a ring.

(a) $R[x]$ is a ring.

(b) $R[x]$ is unital if and only if R is unital; and in that case we have $1_{R[x]} = (1_R, 0, 0, \ldots)$.

(c) The map $\theta\colon R \to R[x]$, $\alpha \mapsto (\alpha, 0, 0, 0, \ldots)$ is an injective homomorphism, so R is isomorphic to the subring of constant polynomials $\theta(R) = \{(\alpha, 0, 0, 0, \ldots)\colon \alpha \in R\}$.

(d) $R[x]$ is commutative if and only if R is commutative.

Proposition 25. If R is a ring and $f, g \in R[x]$ are non-zero, then

(a) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$ (provided $f+g \neq 0$); and

(b) $\deg(fg) \leq \deg(f) + \deg(g)$ (provided $fg \neq 0$).

Proposition 26. Let R be a ring. If $\alpha \in R$ and $f = \sum_{i=0}^{n} a_i x^i \in R[x]$, then let $f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$. The map $\varepsilon_\alpha\colon R[x] \to R$, $f \mapsto f(\alpha)$ is a homomorphism.

Proposition 27. Let R be an integral domain.

(a) If u and v are units of R, then u is an associate of v.

(b) If u is a unit of R and $b \in R$, then $u|b$.

Proposition 28. Let R be an integral domain. If $a, b \in R$, then a and b are associates if and only if $a = bu$ for some unit $u \in R$.

Proposition 29. The relation $\parallel$ given by

$$a \parallel b \iff a \text{ and } b \text{ are associates}$$

is an equivalence relation on an integral domain R.

Proposition 30. If $a \parallel a'$ and $b \parallel b'$, then $a|b \iff a'|b'$.

Theorem 31 (Gauss' lemma)**.** If R is a unique factorisation domain, then so is the polynomial ring $R[x]$.

Proposition 32. Let R be an integral domain and let $a, b \in R$. If d_1 and d_2 are gcds of a and b, then $d_1 \parallel d_2$.

Lemma 33. Let R be a unique factorisation domain and let $a, b \in R$ be non-zero and non-units in R. Write $a = p_1 p_2 \dots p_n$ where each p_i is an irreducible element of R. Then

$$b|a \iff b \parallel c \text{ where } c \text{ is a product of some of } p_1, p_2, \dots, p_n.$$

Theorem 34. If R is a unique factorisation domain then for any $a, b \in R$, there is a gcd of a and b in R.

Proposition 35. Let R be a commutative unital ring. If $a_1, a_2, \dots, a_n \in R$ then the set

$$\langle a_1, a_2, \dots, a_n \rangle = \{a_1 x_1 + a_2 a_2 + \cdots + a_n x_n \colon x_1, \dots, x_n \in R\}$$

is the smallest ideal of R containing $a_1, a_2, \dots, a_n$.

Proposition 36. Let R be an integral domain. For $a, b \in R$, the following are equivalent:

(a) $a|b$

(b) $b \in \langle a \rangle$

(c) $\langle b \rangle \subseteq \langle a \rangle$

Corollary 37. If R is an integral domain and $a, b \in R$, then

$$a \parallel b \iff \langle b \rangle = \langle a \rangle.$$

Proposition 38. If R is an integral domain and $a, b, d \in R$ with $\langle a, b \rangle = \langle d \rangle$, then d is a gcd of a and b.

Proposition 39. If R is a principal ideal domain and $a, b \in R$, then

(a) For any $d \in R$, $\langle a, b\rangle = \langle d\rangle \iff d$ is a gcd of a and b.

(b) a and b have a gcd in R.

(c) If $c \in R$ and d is a gcd of a and b, then the equation

$$ax + by = c$$

has a solution $x, y \in R$ if and only if $d|c$.

Theorem 40. Let R be a principal ideal domain and suppose that $I_1, I_2, I_3, \ldots$ are ideals of R with $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$. Then there is $n \geq 1$ so that $I_n = I_{n+1} = I_{n+2} = \ldots$.

Corollary 41. If R is a principal ideal domain and $a \in R$ with $a \neq 0$ and $a \notin \text{Units}(R)$, then there are $p_1, \ldots p_n \in \text{Irred}(R)$ such that $a = p_1 \ldots p_n$.

Lemma 42. Let R be an integral domain and let $p \in \text{Irred}(R)$.

(a) If $c \in R$ then $c|p \iff c \parallel 1$ or $c \parallel p$.

(b) If $a \in R$ and $p \not| a$ then 1 is a gcd of a and p.

Proposition 43. Let R be a principal ideal domain and let p be an irreducible element of R.

(a) If $a, b \in R$ and $p|ab$, then $p|a$ or $p|b$.

(b) If $a_1, \ldots, a_n \in R$ and $p|a_1 \ldots a_n$, then $p|a_i$ for some $i \in \{1, 2, \ldots, n\}$.

Lemma 44. If R is an integral domain and $p, q \in \text{Irred}(R)$, then $p|q \iff p \parallel q$.

Corollary 45. If R is a principal ideal domain and $p_1, \ldots, p_n$ and $q_1, \ldots, q_m$ are irreducible elements of R with $p_1 \ldots p_n = q_1 \ldots q_m$, then $n = m$ and up to reordering, $p_i \parallel q_i$ for $1 \leq i \leq n$.

Corollary 46. Any principal ideal domain is a unique factorisation domain.

Proposition 47. If F is a field, and f and g are non-zero polynomials in $F[x]$, then there exist polynomials q and r in $F[x]$ so that

$$f = gq + r \quad \text{and} \quad \text{either } r = 0, \text{ or } r \neq 0 \text{ and } \deg(r) < \deg(g).$$

Theorem 48. Let R be a ring. If R is a Euclidean domain, then R is a principal ideal domain.

Proposition 49. Let R be an integral domain. If $a, b \in R$, let $\mathrm{CDivs}(a,b) = \{c \in R : c|a \text{ and } c|b\}$, the set of common divisors of a and b, and let $\mathrm{Gcds}(a,b) = \{c \in R : c \text{ is a gcd of } a \text{ and } b\}$.

(a) If $a, b, s, t \in R$ and $\mathrm{CDivs}(a,b) = \mathrm{CDivs}(s,t)$ then $\mathrm{Gcds}(a,b) = \mathrm{Gcds}(s,t)$.

(b) If c is a gcd of a and b, then $\mathrm{Gcds}(a,b) = \{\text{associates of } c\}$.

Proposition 50. Let R be an integral domain. If $a, b, q, r \in R$ and $a = bq + r$, then $\mathrm{CDivs}(a,b) = \mathrm{CDivs}(b,r)$ and $\mathrm{Gcds}(a,b) = \mathrm{Gcds}(b,r)$.

Proposition 51. Let R be an integral domain. If $a \in R$ then a is a gcd of a and 0_R.

The Euclidean algorithm Let R be a Euclidean domain with Euclidean function $d : R^\times \to \mathbb{N}_0$ and let $a_1, b_1 \in R$. Start with $i = 1$, and then:

(1) If $b_i = 0$ then output a_i and stop.

(2) Otherwise, write $a_i = b_i q_i + r_i$ for some $q_i, r_i \in R$ with either $r_i = 0$, or $r_i \neq 0$ and $d(r_i) < d(b_i)$. Take $a_{i+1} = b_i$ and $b_{i+1} = r_i$, increment i and go back to step (1).

Theorem 52. If R is a Euclidean domain, then the Euclidean algorithm always terminates, and outputs a gcd of the input values a_1 and b_1.

Proposition 53. If a_i, b_i are as in the Euclidean algorithm then there are $x_i, y_i \in R$ with $a_i = a_1 x_i + b_1 y_i$, and we can compute x_i and y_i explicitly.

Theorem 54. If R is an integral domain, then there is a field F which is a field of fractions for R.

Proposition 55. Let R be a commutative unital ring. Then R is a field if and only if $\{0\}$ and R are the only ideals of R.

Theorem 56. If R is a commutative unital ring and $I \lhd R$, then R/I is a field if and only if I is a maximal ideal of R.

Lemma 57. If R is an integral domain and $a \in R$, then

$$a \in \text{Units}(R) \iff \langle a \rangle = R.$$

Theorem 58. Let R be a principal ideal domain. If $I \lhd R$ with $I \neq \{0\}$, then I is a maximal ideal if and only if $I = \langle a \rangle$ for some $a \in \text{Irred}(R)$.

Corollary 59. If F is a field and $f \in F[x]$, then $F[x]/\langle f \rangle$ is a field if and only if $f \in \text{Irred}(F[x])$.

Theorem 60. Let F be a field. If $f \in \text{Irred}(F[x])$ then there is a field extension K of F and $\alpha \in K$ so that $f(\alpha) = 0$. In fact, we can take $K = F[x]/\langle f \rangle$ and $\alpha = \langle f \rangle + x$.

Corollary 61. If $g \in F[x]$ is any polynomial, then there is a field extension K of F, and $\alpha \in K$ so that $g(\alpha) = 0$.

Lemma 62. If $f \in \text{Irred}(F[x])$ and K is a field extension of F containing an element $\alpha \in K$ with $f(\alpha) = 0$, then for $g \in F[x]$ we have $g(\alpha) = 0 \iff g \in \langle f \rangle$.

Theorem 63. If $f \in \text{Irred}(F[x])$ and K is a field extension of F containing an element $\alpha \in K$ with $f(\alpha) = 0$, then K is a field extension of $F[x]/\langle f \rangle$.

Theorem 64. If $f \in \text{Irred}(F[x])$ and $n = \deg(f)$, and $\alpha = \langle f \rangle + x \in F[x]/\langle f \rangle$, then every $y \in F[x]/\langle f \rangle$ can be written as

$$y = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

for a unique choice of $b_0, b_1, \ldots, b_{n-1} \in F$. Hence

$$F[x]/\langle f \rangle = \{r(\alpha) \colon r \in F[x],\ r = 0 \text{ or } r \neq 0 \text{ and } \deg(r) < n\}.$$

Corollary 65. If $p \in \mathbb{N}$ is prime and $f \in \text{Irred}(\mathbb{Z}_p[x])$, then $\mathbb{Z}_p[x]/\langle f \rangle$ is a finite field of order p^n, where $n = \deg(f)$.

Lemma 66. Let L be a field.

(a) If $\mathcal{K}$ is a non-empty family of subfields of L, then $\bigcap \mathcal{K}$ is a subfield of L.

(b) If F is a subfield of L and $S \subseteq L$, then

$$F(S) = \bigcap \{L \colon L \text{ is a subfield of } K \text{ with } F \cup S \subseteq L\}$$

is the smallest subfield of L containing $F \cup S$.

Lemma 67. If $f \in F[x]$ and $f \neq 0$ then there is a unique polynomial $m \in F[x]$ so that m is monic and $m \| f$.

Proposition 68. If K is a field extension of F and $\alpha \in K$, and α is algebraic over F, then there is a unique monic polynomial $m_\alpha \in F[x]$ so that for every $f \in F[x]$ with $f \neq 0$, we have

$$f(\alpha) = 0 \iff m_\alpha | f.$$

We call m_α the *minimum polynomial of α over F*. Moreover, $m_\alpha \in \text{Irred}(F[x])$ and $F(\alpha) \approx F[x]/\langle m_\alpha \rangle$.

Proposition. If $K : F$ then K is a vector space over F, where vector addition is given by addition in K, and scalar addition is given by multiplication in K (after identifying F with a subfield of K).

Theorem 69. Let $K : F$ and suppose that $\alpha \in K$ is algebraic over F, and let m_α be the minimum polynomial of α over F. Then the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ over F, where $n = \deg(m_\alpha)$, and so

$$[F(\alpha) : F] = \deg(m_\alpha).$$

Theorem 70 (The Tower Law)**.** If $L : K$ and $K : F$ then

$$[L : F] = [L : K] \cdot [K : F].$$

Theorem 71. If $P = (x, y)$ is a constructible point in the plane, then $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^k$ for some $k \in \mathbb{N}_0$.

Corollary 72 (Impossibility of duplicating the cube)**.** The point $(\sqrt[3]{2}, 0)$ is not constructible.

Corollary 73 (Impossibility of squaring the circle)**.** The point $(\frac{1}{\sqrt{\pi}}, 0)$ is not constructible.

Lemma 74. The polynomial $x^3 - 3x - 1$ is in $\mathrm{Irred}(\mathbb{Q}[x])$.

Corollary 75 ($\frac{\pi}{3}$ cannot be trisected with a ruler and compasses)**.** The point $(\cos(\frac{\pi}{3}), \sin(\frac{\pi}{3}))$ is not constructible.

Theorem 76. The set $\mathbb{K} = \{x \in \mathbb{R} : (x, 0) \text{ is constructible}\}$ is a subfield of $\mathbb{R}$ with $\mathbb{Q} \subseteq \mathbb{K}$. Moreover, if $x \in \mathbb{K}$ with $x > 0$ then $\sqrt{x} \in \mathbb{K}$.