

Algebra

Sayan Das (dassayan0013@gmail.com)

June 15, 2024

Unit-1

Theory of equations: Relation between roots and coefficients, transformation of equation, Descartes rule of signs, cubic and biquadratic equation. Inequalities, weighted A.M.-G.M.-H.M. inequality, Cauchy-Schwarz inequality.

Unit-2

Definition and examples of groups including permutation groups, dihedral groups and quaternion groups. Elementary properties of groups. Subgroups and examples of subgroups, centraliser, normaliser, center of a group, product of two subgroups.

Unit-3

Properties of cyclic groups, classification of subgroups of cyclic groups. Cycle notation for permutations, properties of permutations, even and odd permutations, alternating group, properties of cosets, Lagrange's theorem and consequences including Fermat's Little theorem.

Unit-4

External direct product of a finite number of groups, normal subgroups, quotient groups, Cauchy's theorem for finite abelian groups. Group homomorphisms, properties of homomorphisms, properties of isomorphisms. First isomorphism theorem, Cayley's theorem.

Unit-5

Definition and examples of rings, properties of rings, subrings, integral domains and fields, characteristic of a ring. [50]

Contents

1	Classical Algebra	3
1.1	Theory of equations	3
1.1.1	The Fundamental Theorem of Algebra	3
1.1.2	Descartes' rule of signs	7
1.1.3	Transformation of Equations	8
1.1.4	Cubics	9
1.1.5	Quartics	12
1.1.6	Exercises	12
1.2	Inequalities	13
2	Groups and Monoids	16
2.1	Definitions and motivation	16
2.2	Permutations	19

2.3	Abstract groups and monoids	22
2.4	Isomorphism and Cayley's theorem	25
2.5	Subgroups and submonoids generated by a subset and cyclic groups . . .	26
2.6	Orbits and cosets	26
2.7	Congruences, quotient monoids and groups	26
2.8	Homomorphisms	26
2.9	Exercises	27
3	Rings	28
3.1	Definition and elementary properties	28
3.2	Integral domains, division rings and fields	29
3.3	Subrings and subfields	29
3.4	Exercises	30

§1 Classical Algebra

§1.1 Theory of equations

§1.1.1 The Fundamental Theorem of Algebra

Remark. When we speak of "a polynomial" we shall mean a *univariate polynomial* (usually in x) unless stated otherwise.

The set of all polynomials in x with coefficients over a field \mathbb{F} is denoted by $\mathbb{F}[x]$, and it forms a *Euclidean domain* with the degree of any $f \in \mathbb{F}[x]$ being the norm $\deg(f)$ (which we will define in the section on ring theory). In particular, if $f, g \in \mathbb{F}[x]$ then

$$\deg(f \circ g) = \deg(f) + \deg(g).$$

We consider $f \in \mathbb{R}[x]$ with $\deg(f) = n$, of the form

$$f(x) = \sum_{j=0}^n a_j x^{n-j} = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n.$$

We say $\alpha \in \mathbb{C}$ is a root of f iff $f(\alpha) = 0$. Suppose $(\alpha_i)_{i=1}^n$ are the roots of f , then

$$f(x) = a_0 \prod_{i=1}^n (x - \alpha_i) = a_0 (x - \alpha_1) \cdots (x - \alpha_n).$$

Note that we haven't assumed the roots α_i to be distinct; the number of times a particular root α_i repeats in the sequence $(\alpha_i)_{i=1}^n$ is called the *multiplicity* of α_i .

Definition 1.1 (Algebraically closed)

We say a field \mathbb{F} is **algebraically closed** iff every non-constant polynomial in $\mathbb{F}[x]$ has a root in \mathbb{F} .

Remark. We saw in Real Analysis that the field of rationals \mathbb{Q} is not complete: in particular, there is no solution to the polynomial equation $x^2 - 2 = 0$ in \mathbb{Q} . The field of reals \mathbb{R} comes about as a completion of the rationals, with the least upper bound property of the reals allowing us to solve equations such as $x^2 - 2 = 0$.

Similarly, we find that the polynomial equation $x^2 + 1 = 0$ has no solutions in \mathbb{R} . We thus say that \mathbb{R} , and certainly also \mathbb{Q} , are not algebraically closed. In order to solve $x^2 + 1 = 0$ we need the field of complex numbers \mathbb{C} due to its following nice property.

Theorem 1.1 (Fundamental Theorem of Algebra)

\mathbb{C} is algebraically closed.

Proof. This proof is due to Fefferman. To show that \mathbb{C} is algebraically closed, consider an arbitrary polynomial $P \in \mathbb{C}[z] : P(z) = \sum_{j=0}^n a_j z^{n-j}$. Then it suffices to show that P has a zero. First we show that $|P(z)|$ attains a maximum as z varies over the entire complex plane, and next that if $|P(z_0)|$ is the minimum of $|P(z)|$, then $P(z_0) = 0$.

Since $|P(z)| = |z|^n \left| \sum_{j=0}^n a_j z^{-j} \right|$ ($z \neq 0$) we can find an $M > 0$ so large that

$$|z| > M \implies |P(z)| \geq |a_n| \quad (1)$$

whilst the continuous function $|P(z)|$ attains a minimum as z varies over the compact disc $\{z \in \mathbb{C} : |z| \leq M\}$. Suppose, then, that

$$|z| \leq M \implies |P(z)| \geq |P(z_0)|. \quad (2)$$

In particular, $P(z_0) \leq P(0) = |a_n|$ so that, by (1), $|z| > M \implies |P(z_0)| \leq |P(z)|$ and using (2) we thus get that

$$|P(z)| \geq |P(z_0)| \quad (\forall z \in \mathbb{C}). \quad (3)$$

Since $P(z) = P((z - z_0) + z_0)$ we may write $P(z)$ as a sum of powers of $z - z_0$, so that for some polynomial $Q \in \mathbb{C}[z]$,

$$P(z) = Q(z - z_0). \quad (4)$$

By (3) and (4),

$$|Q(z)| \geq |Q(0)| \quad (\forall z \in \mathbb{C}). \quad (5)$$

By (4) $P(z_0) = Q(0)$ so it suffices to show that $Q(0) = 0$. Let k be the smallest nonzero exponent for which z^k has a nonzero coefficient in Q . Then we can write

$$\begin{aligned} Q(z) &= c_n + c_{n-k}z^k + \sum_{j=k+1}^n c_{n-j}z^j \quad (c_{n-k} \neq 0) \\ \implies \exists R \in \mathbb{C}[z] : Q(z) &= c_n + c_{n-k}z^k + z^{k+1}R(z) \quad (c_{n-k} \neq 0). \end{aligned} \quad (6)$$

Set $-c_n/c_{n-k} = re^{i\theta}$ and $z_1 = r^{1/k}e^{i\theta/k}$, then

$$c_{n-k}z_1^k = -c_n. \quad (7)$$

Let $\varepsilon > 0$ be arbitrary, then by (6),

$$Q(\varepsilon z_1) = c_n + c_{n-k}\varepsilon^k z_1^k + \varepsilon^{k+1}z_1^{k+1}R(\varepsilon z_1). \quad (8)$$

Since polynomials are bounded on finite discs, we can find an $N > 0$ so large that, for $0 < \varepsilon < 1$, $|R(\varepsilon z_1)| \leq N$. Then, by (7) and (8) we have, for $0 < \varepsilon < 1$,

$$\begin{aligned} |Q(\varepsilon z_1)| &\leq \left| c_n + c_{n-k}\varepsilon^k z_1^k \right| + \varepsilon^{k+1} |z_1|^{k+1} |R(\varepsilon z_1)| \\ &\leq \left| c_n + \varepsilon^k (c_{n-k}z_1^k) \right| + \varepsilon^{k+1} (|z_1|^{k+1} N) \\ &= \left| c_n - c_n \varepsilon^k \right| + \varepsilon^{k+1} (|z_1|^{k+1} N) \end{aligned}$$

$$\begin{aligned}
 &= |c_n| (1 - \varepsilon^k) + \varepsilon^{k+1} (|z_1|^{k+1} N) \\
 &= |c_n| - \varepsilon^k |c_n| + \varepsilon^{k+1} (|z_1|^{k+1} N)
 \end{aligned} \tag{9}$$

If $c_n \neq 0$, then take ε so small that $\varepsilon^{k+1} (|z_1|^{k+1} N) < \varepsilon^k |c_n|$. Thus, by (9)

$$|Q(\varepsilon z_1)| \leq |c_n| - \varepsilon^k |c_n| + \varepsilon^{k+1} (|z_1|^{k+1} N) < |c_n| - \varepsilon^k |c_n| + \varepsilon^k |c_n| = |c_n| = |Q(0)|$$

which contradicts (5). So $|c_n| = 0$ and thus $Q(0) = c_n = 0$. \square

Theorem 1.2

The following are equivalent:

1. The field of complex numbers is algebraically closed.
2. Every non-constant polynomial with complex coefficients has a complex root.
3. Every nonzero polynomial of degree n with complex coefficients has exactly n complex roots.

Proof. (1.) \iff (2.) by definition. Now to show (2.) \iff (3.). That (3.) \implies (2.) is obvious, so we show (2.) \implies (3.). Suppose $f \in \mathbb{C}[x] : f(x) = \sum_{j=0}^n a_j x^{n-j}$ with $\deg(f) = n$ (so $a_0 \neq 0$). Then using (2.) there exists $\alpha_1 \in \mathbb{C} : f(\alpha_1) = 0$, so by the factor theorem for polynomials $(x - \alpha_1)$ is a factor of f i.e. $f(x) = (x - \alpha_1)f_1(x)$ for some $f_1 \in \mathbb{C}[x] : \deg(f_1) = n - 1$ with leading coefficient a_0 .

Again, using (2.) there exists $\alpha_2 \in \mathbb{C} : f_1(\alpha_2) = 0$ and again by the factor theorem $f_1(x) = (x - \alpha_2)f_2(x)$ for some $f_2 \in \mathbb{C}[x] : \deg(f_2) = n - 2$ with leading coefficient a_0 . In this way we get $f_{k-1}(x) = (x - \alpha_k)f_k(x)$ for $k = 2, \dots, n$ with $\deg(f_k) = n - k$, $\alpha_k \in \mathbb{C}$. Then $\deg(f_n) = 0 \implies f_n$ is the constant function $f_n(x) = a_0$ so that $f_{n-1}(x) = (x - \alpha_n)a_0$.

Thus, we have $f(x) = (x - \alpha_1)f_1(x)$

$$\begin{aligned}
 &= (x - \alpha_1)(x - \alpha_2)f_2(x) \\
 &= (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)f_n(x) \\
 &= (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)a_0 \\
 \therefore f(x) &= a_0(x - \alpha_1) \cdots (x - \alpha_n) = a_0 \prod_{j=1}^n (x - \alpha_j).
 \end{aligned}$$

Now suppose there exists $\beta \in \mathbb{C} : f(\beta) = 0$ and $\beta \neq \alpha_j$ for $j = 1, \dots, n$. Then

$$f(\beta) = a_0 \prod_{j=1}^n (\beta - \alpha_j) = 0$$

$$(a_0 \neq 0) \implies \beta = \alpha_j \quad \forall j = 1, \dots, n.$$

An absurdity. This means that $(\alpha_j)_{j=1}^n$ are all the possible zeros of f , so f has exactly n zeros. \square

Theorem 1.3 (Complex conjugate root theorem)

If $f \in \mathbb{R}[x] : f(\zeta) = 0$ for some $\zeta \in \mathbb{C}$, then $f(\bar{\zeta}) = 0$.

Proof. Let $f(x) = \sum_{j=0}^n a_{n-j}x^j$ with each $a_{n-j} \in \mathbb{R}$. Then, $f(\zeta) = 0$

$$\begin{aligned} \implies \sum_{j=0}^n a_{n-j}\zeta^j &= 0 \\ \implies \overline{\sum_{j=0}^n a_{n-j}\zeta^j} &= \bar{0} \\ \implies \sum_{j=0}^n \overline{a_{n-j}\zeta^j} &= 0 \\ \implies \sum_{j=0}^n a_{n-j}\bar{\zeta}^j &= 0 \\ \implies \sum_{j=0}^n a_{n-j}\bar{\zeta}^j &= f(\bar{\zeta}) = 0. \end{aligned}$$

Thus, $f(\bar{\zeta}) = 0$. □

Remark. The above proof only worked because all the coefficient were real, so $a_{n-k} = \overline{a_{n-k}}$. Indeed, the complex conjugate root theorem is not necessarily true for $f \in \mathbb{C}[x]$.

Theorem 1.4 (Conjugate radical root theorem)

If $P \in \mathbb{Q}[x] : P(s + t\sqrt{u}) = 0$ for some $s, t, u \in \mathbb{Q}$, $\sqrt{u} \notin \mathbb{Q}$, then $P(s - t\sqrt{u}) = 0$.

Proof. Put $Q(x) = P(s + tx) = \sum b_k x^k$. Clearly, the b_k are rational, and $Q(\sqrt{u}) = 0$. We have

$$Q(\sqrt{u}) = \sum_{2|k} b_k u^{k/2} + \sqrt{u} \sum_{2 \nmid k} b_k u^{(k-1)/2} = A + \sqrt{u}B.$$

Now as A, B are rationals and \sqrt{u} not, we must have $A = B = 0$, and hence $Q(-\sqrt{u}) = A - \sqrt{u}B = 0$, and we are done. □

Remark. Viète found the following identities relating the roots of a polynomial with its coefficients.

Lemma 1.1 (Viète's relations)

If $f \in \mathbb{C}[x] : f(x) = a_0 \prod_{i=1}^n (x - \alpha_i) = \sum_{j=0}^n a_j x^{n-j}$, ($a_0 \neq 0$) and

$$\sigma_1 = \sum_{1 \leq i \leq n} \alpha_i, \quad \sigma_2 = \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j, \quad \dots, \quad \sigma_n = \prod_{1 \leq i \leq n} \alpha_i$$

with

$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} \left(\prod_{1 \leq i \leq k} \alpha_{i_i} \right)$$

in general, then:

$$\sigma_1 = -\frac{a_1}{a_0}, \quad \dots, \quad \sigma_k = (-1)^k \frac{a_k}{a_0}, \quad \dots, \quad \sigma_n = (-1)^n \frac{a_n}{a_0}$$

Proof Sketch. Observe that

$$f(x) = \sum_{j=0}^n a_j x^{n-j} = 0$$

$$\iff x^n + \sum_{j=1}^n \frac{a_j}{a_0} x^{n-j} = 0$$

and

$$f(x) = a_0 \prod_{i=1}^n (x - \alpha_i) = 0$$

$$\iff \prod_{i=1}^n (x - \alpha_i) = 0$$

$$\iff x^n - (\alpha_1 + \dots + \alpha_n)x^{n-1} + (\alpha_1\alpha_2 + \dots + \alpha_{n-1}\alpha_n)x^{n-2} + \dots + (-1)^n(\alpha_1 \dots \alpha_n) = 0$$

$$\iff x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \dots + (-1)^k \sigma_k x^{n-k} + \dots + (-1)^n \sigma_n$$

$$= x^n + \sum_{k=1}^n (-1)^k \sigma_k x^{n-k} = 0$$

$$\text{thus } \sigma_k = (-1)^k \frac{a_k}{a_0}.$$

□

Remark. Observe that the above relations are all polynomials in the roots $(\alpha_i)_{i=1}^n$ of the polynomial $f(x)$; moreover they are symmetric with respect to the roots $(\alpha_i)_{i=1}^n$, i.e., the relations remain invariant under any permutation of the roots. We call these σ_i 's *elementary symmetric polynomials*. We will study symmetries in general in group theory.

Before concluding this section we note that it is often easier to work with monic polynomials (polynomials having leading coefficient of 1). So we often divide by the leading coefficient:

$$a_0 x^n + \dots + a_{n-1} x + a_n = 0 \iff x^n + \dots + \frac{a_{n-1}}{a_0} x + \frac{a_n}{a_0} = 0 \quad (a_0 \neq 0).$$

$$\iff x^n + \dots + b_1 x + b_0 = 0$$

where $b_i = \frac{a_{n-i}}{a_0}$.

§1.1.2 Descartes' rule of signs

Fact 1.1

We consider $f \in \mathbb{R}[x] : f(x) = \sum_{j=0}^n a_j x^{n-j}$.

The number of positive roots of $f(x) = 0$ does not exceed the number of variations signs in the sequence $(\text{sgn}(a_j))_{j=0}^n$ of the signs of the coefficients of $f(x)$, and if less it is less by an even number.

Consequently, we also have that the number of negative roots of $f(x) = 0$ does not exceed the number of variations of signs in the sequence

$$(\text{sgn}(b_j))_{j=0}^n = (\text{sgn}((-1)^j a_j))_{j=0}^n$$

of the signs of the coefficients of $f(-x)$, and if less it is less by an even number.

Example 1.1

Let $f(x) = 5x^6 - 7x^4 + x^2 - 7x + 8$, then $f(-x) = 5x^6 - 7x^4 + x^2 + 7x + 8$.

The sequence of signs of the coefficients of $f(x)$ is $(+1, -1, +1, -1, +1)$. There are 4 variations so the no. of positive roots of $f(x) = 0$ is 0, 2 or 4.

The sequence of signs of the coefficients of $f(-x)$ is $(+1, -1, +1, +1, +1)$. There are 2 variations so the no. of negative roots of $f(x) = 0$ is 0 or 2.

$\deg(f) = 6$ means that it has 6 complex roots by the Fundamental Theorem of Algebra. So the number of non-real complex roots can be 0, 2, 4, or 6 by the complex conjugate root theorem. So we can summarise the nature of the roots of $f(x)$ as follows:

Positive real	Negative real	Non-real complex
4	2	0
4	0	2
2	2	2
2	0	4
0	2	4
0	0	6

§1.1.3 Transformation of Equations

Remark. Given a polynomial equation it is possible, without knowing the roots, to obtain a new equation whose roots are connected with those of the original equation by some assigned relation. The method of finding this new equation is called a transformation. Such a transformation is occasionally useful for studying the nature of the roots of the given polynomial which might have proved difficult otherwise.

In general, given a polynomial equation $f(x) = 0 : f \in \mathbb{F}[x]$, we are to obtain another polynomial equation $\varphi(y) = 0 : \varphi \in \mathbb{F}[x]$ whose roots are connected with the roots of $f(x)$ by some relation $\psi(x, y) = 0$.

We obtain $\varphi(y) = 0$ by eliminating x between $f(x) = 0$ and $\psi(x, y) = 0$.

§1.1.4 Cubics

Remark. We already know how to solve quadratic equations of the form $ax^2 + bx + c = 0$ by completing the square:

$$\begin{aligned} ax^2 + bx + c &= a(x + bH)^2 - ab^2H^2 + c \\ \implies ax^2 + bx + c &= ax^2 + 2abHx + ab^2H^2 - (ab^2H^2 - c) \\ \therefore H &= \frac{1}{2a}, \quad a\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a} = 0 \end{aligned}$$

and consequently

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

A corollary of the quadratic formula is:

Lemma 1.2

Given any $M, N \in \mathbb{C}$, there exist $g, h \in \mathbb{C} : g + h = M$ and $gh = N$; moreover, g and h are the roots of $x^2 - Mx + N$.

Proof. The quadratic formula provides roots g and h of $x^2 - Mx + N$. Now,

$$x^2 - Mx + N = (x - g)(x - h) = x^2 - (g + h)x + gh$$

and so $g + h = M$ and $gh = N$. □

Remark. Arising from a tradition of public mathematics contests in Venice and Pisa, methods to solve equations of degree 3 (cubics) and 4 (quartics/biquadratics) were found in the early 1500s by del Ferro, Tartaglia, Ferrari and Cardano.

We now derive the general formula for the roots of a cubic. The change of variable $X = x - \frac{b}{3a}$ transforms the cubic $f(X) = aX^3 + bX^2 + cX + d$ into a simpler cubic polynomial $f(x)$ with no quadratic terms:

$$\begin{aligned} F\left(x - \frac{b}{3a}\right) &= f(x) = ax^3 + \frac{(3ac - b^2)}{3a}x + \frac{2b^3 - 9abc + 27a^2d}{27a^2} \\ &= x^3 + \underbrace{\frac{(3ac - b^2)}{3a^2}}_q x + \underbrace{\frac{2b^3 - 9abc + 27a^2d}{27a^3}}_r \\ &= x^3 + qx + r \end{aligned}$$

So, $F\left(x - \frac{b}{3a}\right) = f(x) = x^3 + qx + r$.

Theorem 1.5 (Cubic Formula)

The roots of $f \in \mathbb{R}[x] : f(x) = x^3 + qx + r$ are

$$\alpha_1 = g + h, \quad \alpha_2 = \omega g + \omega^2 h, \quad \alpha_3 = \omega^2 g + \omega h,$$

where $g^3 = \frac{1}{2}(-r + \sqrt{R})$, $h = -q/3g$, $R = r^2 + \frac{4}{27}q^3$ and $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ is a

primitive cube root of unity. Moreover,

$$\begin{cases} R > 0 \implies & \text{one real root, two complex conjugate roots} \\ R = 0 \implies & \text{three real roots, at least two equal} \\ R < 0 \implies & \text{three distinct real roots} \end{cases}$$

Proof. Write a root u of $f(x) = x^3 + qx + r$ as

$$u = g + h,$$

where g and h are to be chosen, and substitute:

$$\begin{aligned} 0 &= f(u) = f(g + h) \\ &= (g + h)^3 + q(g + h) + r \\ &= g^3 + h^3 + 3gh(g + h) + q(g + h) + r \\ &= g^3 + h^3 + (3gh + q)u + r. \end{aligned}$$

If $3gh + q = 0$ then $gh = -q/3$. By Lemma (1.2), given u , $-q/3 \in \mathbb{C}$ there exist $g, h \in \mathbb{C} : g + h = u$ and $gh = -q/3$; this choice forces $3gh + q = 0$, so that $g^3 + h^3 = -r$. Cubing both sides of $gh = -q/3$ we get

$$\begin{cases} g^3 + h^3 = -r, \\ g^3 h^3 = -q^3/27. \end{cases}$$

By Lemma (1.2), there is a quadratic in g^3 :

$$g^6 + rg^3 - q^3/27 = 0.$$

The quadratic formula gives

$$g^3 = \frac{1}{2} \left(-r + \sqrt{r^2 + \frac{4}{27}q^3} \right) = \frac{1}{2} \left(-r + \sqrt{R} \right)$$

and $h^3 = -r - g^3 = \frac{1}{2} \left(-r - \sqrt{R} \right)$ is also a root of this quadratic. So $g^3 - h^3 = \sqrt{R}$. There are three cube roots of g^3 : g , ωg , and $\omega^2 g$. Due to the constraint $gh = -q/3$, each of these has a "mate": g and $h = -q/(3g)$; ωg and $\omega^2 h = -q/(3\omega g)$; $\omega^2 g$ and $\omega h = -q/(3\omega^2 g)$ (for $\omega^3 = 1$).

When $R < 0$, we have $r^2 + \frac{4}{27}q^3 = -k^2$ so that

$$g^3 = \frac{1}{2} \left(-r + \sqrt{R} \right) = \frac{1}{2} \left(-r + i\sqrt{k} \right), \quad h^3 = \frac{1}{2} \left(-r - \sqrt{R} \right) = \frac{1}{2} \left(-r - i\sqrt{k} \right).$$

Set $-\frac{r}{2} = \rho \cos(\theta)$, $\frac{k}{2} = \rho \sin(\theta)$ where $\theta \in (-\pi, \pi]$. Then

$$g^3 = \rho(\cos(\theta) + i \sin(\theta)) \text{ and } \rho^2 = -\frac{4}{27}q^3$$

so using de Moivre's theorem we get three values of $g =$

$$\sqrt[3]{\rho} \left(\cos \left(\frac{\theta}{3} \right) + i \sin \left(\frac{\theta}{3} \right) \right), \quad \sqrt[3]{\rho} \left(\cos \left(\frac{2\pi + \theta}{3} \right) + i \sin \left(\frac{2\pi + \theta}{3} \right) \right),$$

$$\sqrt[3]{\rho} \left(\cos \left(\frac{4\pi + \theta}{3} \right) + i \sin \left(\frac{4\pi + \theta}{3} \right) \right)$$

and as $gh = -q/3$, corresponding values of h will be $\Re(g) - \Im(g)$; thus in $u = g + h$ the imaginary parts cancel out and we get real roots (as $q < 0$ when $R < 0$)

$$2\sqrt{-\frac{4^{1/3}}{3}q \cos \left(\frac{\theta}{3} \right)}, \quad 2\sqrt{-\frac{4^{1/3}}{3}q \cos \left(\frac{2\pi + \theta}{3} \right)}, \quad 2\sqrt{-\frac{4^{1/3}}{3}q \cos \left(\frac{4\pi + \theta}{3} \right)}.$$

□

Example 1.2

If $f(x) = x^3 - 15x - 126$, then $q = -15$, $r = -126$ and

$$R = r^2 + \frac{4}{27}q^3 = 15876 - 500 = 15376 > 0.$$

Thus, $g^3 = \frac{1}{2}(126 + 124) = 125 \implies g = 5, h = 1$.

So the roots are $x = 6$, $5\omega + \omega^2 = -3 + 2i\sqrt{3}$, $5\omega^2 + \omega = -3 - 2i\sqrt{3}$.

Alternatively, having found one root to be 6, the other two roots can be found as the roots of the quadratic $f(x)/(x - 6) = x^2 + 6x + 21$.

Example 1.3

If $f(x) = x^3 - 7x + 6$, then $q = -7$, $r = 6$, and

$$R = r^2 + \frac{4}{27}q^3 = \frac{972 - 1372}{27} = -\frac{400}{27} < 0$$

$$\begin{aligned} \text{then } g + h &= \sqrt[3]{\frac{1}{2} \left(-6 + i\frac{20\sqrt{3}}{9} \right)} + \sqrt[3]{\frac{1}{2} \left(-6 - i\frac{20\sqrt{3}}{9} \right)} \\ &= \sqrt[3]{\left(-3 + i\frac{10\sqrt{3}}{9} \right)} + \sqrt[3]{\left(-3 - i\frac{10\sqrt{3}}{9} \right)} \\ &= \sqrt{\frac{7}{3}} \left(\cos \left(\frac{\pi - \arctan \left(\frac{10\sqrt{3}}{27} \right)}{3} \right) + i \sin \left(\frac{\pi - \arctan \left(\frac{10\sqrt{3}}{27} \right)}{3} \right) \right) \\ &\quad + \sqrt{\frac{7}{3}} \left(\cos \left(\frac{\pi - \arctan \left(\frac{10\sqrt{3}}{27} \right)}{3} \right) - i \sin \left(\frac{\pi - \arctan \left(\frac{10\sqrt{3}}{27} \right)}{3} \right) \right) \end{aligned}$$

$$= 2\sqrt{\frac{7}{3}} \left(\cos \left(\frac{\pi - \arctan\left(\frac{10\sqrt{3}}{27}\right)}{3} \right) \right) = 2\sqrt{\frac{7}{3}} \left(\sqrt{\frac{3}{7}} \right) = 2.$$

The other two roots are then

$$2\sqrt{\frac{7}{3}} \left(\cos \left(\frac{2\pi + \pi - \arctan\left(\frac{10\sqrt{3}}{27}\right)}{3} \right) \right) = 2\sqrt{\frac{7}{3}} \left(\frac{-3}{2} \sqrt{\frac{3}{7}} \right) = -3,$$

and

$$2\sqrt{\frac{7}{3}} \left(\cos \left(\frac{4\pi + \pi - \arctan\left(\frac{10\sqrt{3}}{27}\right)}{3} \right) \right) = 2\sqrt{\frac{7}{3}} \left(\frac{1}{2} \sqrt{\frac{3}{7}} \right) = 1.$$

Thus, $f(x) = (x-1)(x-2)(x+3)$.

§1.1.5 Quartics

Remark. We conclude this chapter with a discussion of quartic polynomials.

Consider the quartic $F(X) = X^4 + bX^3 + cX^2 + dX + e$ (if it isn't monic we can always transform it into a polynomial that is monic). As before, we do a change of variable $X = x - \frac{1}{4}b$ to get a simpler polynomial

$$F\left(x - \frac{1}{4}b\right) = f(x) = x^4 + qx^2 + rx + s$$

whose roots yield the roots of $F(X)$: if $f(u) = 0$ then $F(u - \frac{1}{4}b) = 0$. The quartic formula was found by Ferrari in the 1540s, but the version we discuss is from the work done by Descartes in 1637. Factorise $f(x)$ into two quadratic terms,

$$f(x) = x^4 + qx^2 + rx + s = (x^2 + jx + \ell)(x^2 - jx + m)$$

§1.1.6 Exercises

Exercise 1.6. Prove that the roots of the following equations are all real.

1. $\sum_{i=1}^n \frac{1}{x + a_i} = \frac{1}{x}, \quad a_i \in \mathbb{R}^+.$
2. $\sum_{i=1}^n \frac{1}{x + a_i} = \frac{1}{x}, \quad a_i \in \mathbb{R}^-.$
3. $\sum_{i=1}^n \frac{1}{x + a_i} = \frac{1}{x + b}, \quad b, a_i \in \mathbb{R}^+, b > a_i.$
4. $\sum_{i=1}^n \frac{1}{x + a_i} = \frac{1}{x + b}, \quad b, a_i \in \mathbb{R}, b < a_i.$
5. $\sum_{i=1}^n \frac{A_i}{x + a_i} = x + b, \quad b, a_i, A_i \in \mathbb{R}, A_i > 0.$

Exercise 1.7. The roots of the equation $x^3 + px^2 + qx + r = 0$, ($r \neq 0$), are α, β, γ . Find the equation whose roots are:

1. $\frac{1}{\alpha} + \frac{1}{\beta} - \frac{1}{\gamma}, \frac{1}{\beta} + \frac{1}{\gamma} - \frac{1}{\alpha}, \frac{1}{\gamma} + \frac{1}{\alpha} - \frac{1}{\beta},$
2. $\alpha\beta + \frac{1}{\gamma}, \beta\gamma + \frac{1}{\alpha}, \gamma\alpha + \frac{1}{\beta},$
3. $\alpha - \frac{\beta\gamma}{\alpha}, \beta - \frac{\gamma\alpha}{\beta}, \gamma - \frac{\alpha\beta}{\gamma},$
4. $\frac{\alpha + \beta}{\gamma}, \frac{\beta + \gamma}{\alpha}, \frac{\gamma + \alpha}{\beta}.$

§1.2 Inequalities

Theorem 1.8 (Triangle Inequality)

If $x, y, z \in \mathbb{R}$, then $\|x + y\| + \|y + z\| \geq \|x + z\|$.

Theorem 1.9 (Arithmetic Mean \geq Geometric Mean \geq Harmonic Mean Inequality)

If a_1, \dots, a_n are arbitrary elements of \mathbb{R} , then

$$\left(\frac{1}{n} \sum_{j=1}^n a_j \right) \geq \left(\prod_{j=1}^n a_j \right)^{\frac{1}{n}} \geq \left(\frac{n}{\sum_{j=1}^n \frac{1}{a_j}} \right).$$

Theorem 1.10 (Cauchy-Schwarz Inequality)

If a_1, \dots, a_n and b_1, \dots, b_n are arbitrary elements of \mathbb{R} , then

$$\left(\sum_{j=1}^n a_j^2 \right) \left(\sum_{j=1}^n b_j^2 \right) \geq \left(\sum_{j=1}^n a_j b_j \right)^2.$$

Moreover, if some $a_i \neq 0$ equality holds iff there is a $\lambda \in \mathbb{F}$ such that $a_j \lambda + b_j = 0$ for all $j = 1, \dots, n$.

Theorem 1.11 (Bernoulli's Inequality)

If $x \in \mathbb{R}$ such that $x \geq -1$, then for every positive integer n

$$(1 + x)^n \geq 1 + nx.$$

Moreover, if $x > -1$ and $x \neq 0$, then $(1 + x)^n > 1 + nx$ for all $n \geq 2$.

Definition 1.2 (Convexity)

A function $f : D_f \rightarrow \mathbb{R}, D_f \subseteq \mathbb{R}$ is **convex** iff $\forall t \in (0, 1)$ and $r, s \in D_f$ we have:

$$f(tr + (1 - t)s) \leq tf(r) + (1 - t)f(s).$$

Also, f is **concave** iff $-f$ is convex.

Theorem 1.12 (Jensen's Inequality)

Let $f : D_f \rightarrow \mathbb{R}, D_f \subseteq \mathbb{R}$ and $\{x_j\}_{j=1}^n \subseteq D_f$ with a_1, \dots, a_n being arbitrary positive reals. If

1. f is **convex** then

$$\frac{\sum_{j=1}^n a_j f(x_j)}{\sum_{j=1}^n a_j} \geq f\left(\frac{\sum_{j=1}^n a_j x_j}{\sum_{j=1}^n a_j}\right).$$

2. f is **concave** then

$$\frac{\sum_{j=1}^n a_j f(x_j)}{\sum_{j=1}^n a_j} \leq f\left(\frac{\sum_{j=1}^n a_j x_j}{\sum_{j=1}^n a_j}\right).$$

Theorem 1.13 (Minkowski's Inequality)

If $p \geq 1$ and x_1, \dots, x_n and y_1, \dots, y_n are arbitrary elements of \mathbb{R} , then

$$\left(\sum_{k=1}^n |x_k|^p\right)^{\frac{1}{p}} + \left(\sum_{k=1}^n |y_k|^p\right)^{\frac{1}{p}} \geq \left(\sum_{k=1}^n |x_k + y_k|^p\right)^{\frac{1}{p}}.$$

Theorem 1.14 (Hölder's Inequality)

If $p, q \geq 1 : 1/p + 1/q = 1$ and x_1, \dots, x_n and y_1, \dots, y_n are arbitrary elements of \mathbb{R} , then

$$\left(\sum_{k=1}^n |x_k|^p\right)^{\frac{1}{p}} \left(\sum_{k=1}^n |y_k|^q\right)^{\frac{1}{q}} \geq \left(\sum_{k=1}^n |x_k + y_k|\right).$$

Theorem 1.15 (Tschebyscheff's Inequality)

If $(a_k)_{k=1}^n, (b_k)_{k=1}^n$ are either both monotonically increasing or both monotonically decreasing sequences in \mathbb{R} , then

$$n \left(\sum_{k=1}^n a_k b_k\right) \geq \left(\sum_{k=1}^n a_k\right) \left(\sum_{k=1}^n b_k\right).$$

Theorem 1.16 (Rearrangement Inequality)

If b_1, \dots, b_n is any rearrangement of the positive reals a_1, \dots, a_n , then:

$$\sum_{i=1}^n \frac{a_i}{b_i} \geq n.$$

Theorem 1.17 (Weierstrass's Inequalities)

If $\sum_{k=1}^n a_k < 1 : a_k \in (0, 1)$ for some arbitrary positive reals a_1, \dots, a_n , then:

$$\frac{1}{1 \mp \sum_{k=1}^n a_k} < \prod_{k=1}^n (1 \pm a_k) < 1 \pm \sum_{k=1}^n a_k.$$

§2 Groups and Monoids

§2.1 Definitions and motivation

Remark. In classical algebra we sought formulas for the roots of a polynomial $f(x)$, involving only radicals and elementary arithmetic operations on the coefficients of $f(x)$ (if such a formula exists we say that $f(x)$ is **solvable by radicals**). We already know the quadratic formula, and have also seen Cardano's and Ferrari's general solutions for the cubic and quartic cases. Naturally the question arises: is there such a formula for the quintic case? Moreover, is there a formula for the roots of polynomials which generalises the quadratic, cubic and quartic formulas - a formula for the roots of any polynomial of degree n ?

Évariste Galois, a young student at the École Normale Supérieure, found an answer, by considering the following object.

Definition 2.1 (Concrete group)

Let X be a set. A **group** G_X is the set of *symmetries* of X .

Remark. A *symmetry* is another name for *permutation*. Why did Galois study permutations? What could they have to do with formulas for roots? The key idea is that formulas involving radicals are necessarily ambiguous. After all, if s is an n^{th} root of a number r i.e. $s^n = r$, then ωs is also an n^{th} root of r (ω being any n^{th} root of unity), for $(\omega s)^n = \omega^n s^n = s^n = r$. Recall also Viète's relations, relating the roots of $f(x)$ in terms of *elementary symmetric polynomials* in its coefficients. So we know that the coefficients of $f(x)$ are *symmetric*, i.e., they are unchanged by permuting the roots of $f(x)$.

In 1799, Ruffini claimed that the general quintic was in fact *unsolvable by radicals*. His proof wasn't accepted, however, as although his general ideas were, in fact, correct, his proof had gaps in it.

In 1815, Cauchy introduced the multiplication of permutations and proved basic properties of what is known as the *symmetric group* S_n .

In 1824, Abel filled the gaps in Ruffini's proof by building on Cauchy's work and constructing permutations of the roots of a quintic, using certain rational functions introduced by Lagrange. We now know the result that there is no general quintic formula as the *Abel-Ruffini Theorem*.

In 1830, Galois, before meeting a tragic but nevertheless romantic end at an early age due to his dueling tendencies, realised the importance of what he called *groups* (subsets of S_n which are closed under composition, which we call *subgroups*) towards understanding which polynomials of any degree are solvable by radicals. He associated each polynomial $f(x)$ with a group, now called the *Galois group* of $f(x)$. He recognised conjugation, normal subgroups, quotient groups, and simple groups, and he proved that any polynomial over a field of characteristic 0 is solvable by radicals iff its Galois group is a *solvable group* (solvability being a property generalising commutativity).

We will not cover everything that Galois did just yet in this course (we will cover more in the courses Group Theory, and Field Theory and Canonical Forms of Matrices). However, we note that since Galois' time, groups have arisen in many areas within and beyond mathematics outside of the study of roots of polynomials, for they are a precise way to describe the notion of symmetry.

Example 2.1

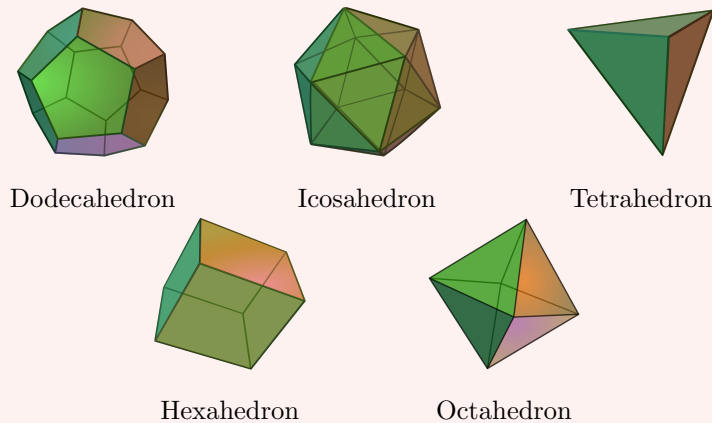
Consider a rectangle, then it has the following symmetries:

1. we do nothing
2. we reflect it horizontally
3. we reflect it vertically
4. we rotate it by π radians

We'll return to the geometric interpretation later, noting that the rectangle has a symmetric group of order 4.

Example 2.2

Consider the five regular Platonic solids. The dodecahedron has symmetries of order 5, 3, 2 and 1. It has 12 faces, so if we pick one face and put it at the bottom, we'd have 5 ways to rotate it about its top-bottom axis. So the total number of symmetries is $5 \times 12 = 60$, which is the order of its symmetric group. If we were to count reflections as well, its symmetric group would be of order 120.



The 5 regular Platonic solids.

We'll return to the notion of symmetric group and alternating group later, noting that the dual polyhedron of the dodecahedron, the icosahedron, also has a symmetric group of order 60, the tetrahedron of order 12, and the hexahedron (cube) and the octahedron of order 24.

Remark. Note that a symmetry can be *noncommutative*: consider the transformations of a hexahedron for example.

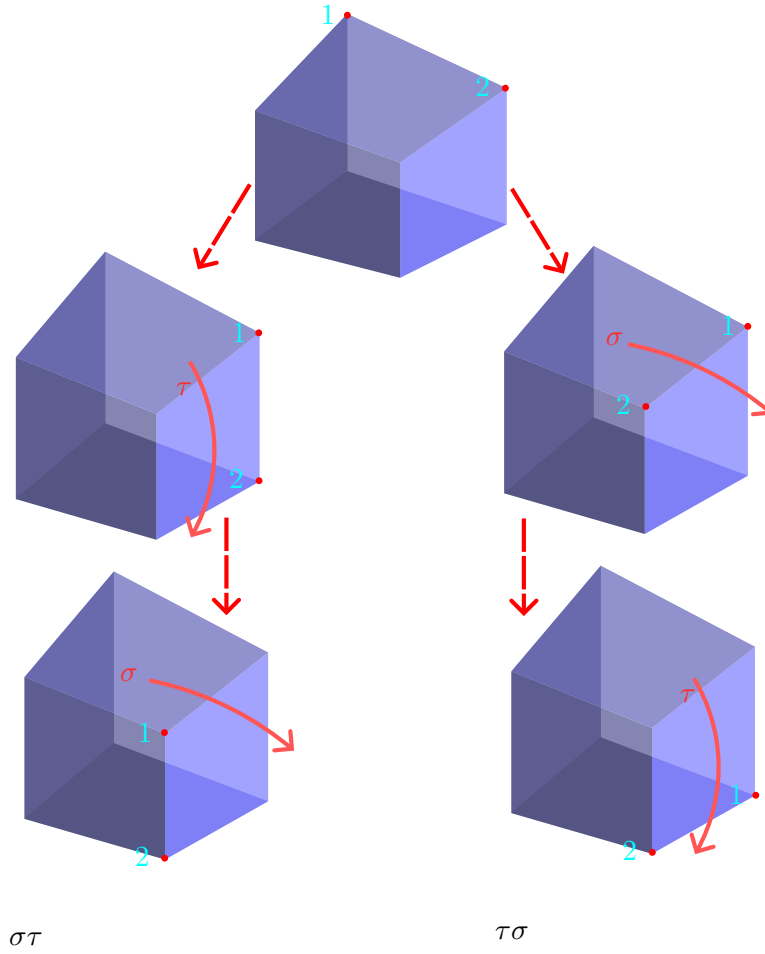


Figure 1: $\sigma\tau \neq \tau\sigma$

So it is natural that we should want some operation in which we consider *ordered pairs*.

Definition 2.2

A **binary operation** on a set R is a function $*$: $R \times R \rightarrow R$, denoted by $(r, r') \mapsto r * r'$.

Remark. As $*$ is a function, it is single-valued; i.e., the **law of substitution** holds: if $r = r'$ and $s = s'$, then $r * s = r' * s'$.

The above shows that $*$ is **well-defined**: the definition of $*$ assigns a unique value $r * s = q \in R$ to every $r, s \in R$; the same $(r, s) \in R \times R$ cannot have multiple different $q, q_1, \dots, q_n \in R$ assigned to it (although the same $q = r * s$ can corespond to multiple different ordered pairs in $R \times R$, so a binary operation need not be injective).

Also note that $r, s \in R \implies r * s \in R$ by definition; we say that R is **closed** under $*$.

We will now make the notion of *permutation* more precise.

§2.2 Permutations

Definition 2.3 (Permutation)

A **permutation** of a set X is a bijection from X to itself.

Remark. A permutation of a finite set X can be viewed as a rearrangement, i.e., as a list with no repetitions of all the elements of X .

Example 2.3 1. The rearrangements of $X = \{1, 2, 3\}$ are :

123; 132; 213; 231; 312; 321.

2. Now let $X = \{1, \dots, n\}$. Then there are exactly $n!$ rearrangements of the n -element set X .

Remark. A rearrangement i_1, i_2, \dots, i_n of X determines a function $\alpha : X \rightarrow X$, namely, $\alpha(1) = i_1, \alpha(2) = i_2, \dots, \alpha(n) = i_n$.

Example 2.4

The rearrangement 213 determines a function α with $\alpha(1) = 2, \alpha(2) = 1$, and $\alpha(3) = 3$.

Notation. We use a two-rowed notation to denote the function corresponding a rearrangement; if $\alpha(j)$ is the j^{th} item on the list, then

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & j & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(j) & \dots & \alpha(n) \end{pmatrix}.$$

Remark. That a list contains all the elements of X says that the correspondence function α is surjective, for the bottom row is $\text{im } \alpha$. That there are no repetitions on the list says that distinct points have distinct values, i.e., α is injective. Thus, every list determines a bijection $\alpha : X \rightarrow X$; i.e., each rearrangement determines a permutation. Conversely, each permutation determines a rearrangement, namely, the list $\alpha(1), \alpha(2), \dots, \alpha(n)$ displayed as the bottom row. Rearrangements are permutations and permutations are rearrangements. The advantage of viewing permutations as functions, however, is that they can be composed.

Notation. We denote the family of all permutations of a set X by S_X , but when $X = \{1, \dots, n\}$ we denote S_X by S_n . The identity permutation is usually denoted (1).

Remark. Composition is a binary operation on S_X : the composite of two permutations is a permutation. Composition in S_3 is *noncommutative*: consider permutations α, β of S_3 such that

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Then,

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Thus $\alpha\beta \neq \beta\alpha$. It follows that composition is noncommutative in $S_n, n \geq 3$. We'll now introduce some special permutations:

Definition 2.4

Let $f : X \rightarrow X$. If $x \in X$ then f **fixes** x iff $f(x) = x$, and f **moves** x iff $f(x) \neq x$. Let i_1, i_2, \dots, i_r be distinct integers in $X = \{1, 2, \dots, n\}$. If $\alpha \in S_n$ fixes the other integers in X (if any) and if

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \dots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1,$$

then α is called an **r -cycle**, or a *cycle of length r* , and we denote it by

$$\alpha = (i_1 \ i_2 \ \dots \ i_r).$$

A 2-cycle $(i_1 \ i_2)$ interchanges i_1 and i_2 and fixes the rest, and so a 2-cycle is also called a **transposition**.

Remark. Cycle comes from the Greek word for circle. The cycle $\alpha = (i_1 \ i_2 \ \dots \ i_r)$ can be visualised as a clockwise rotation of the circle:

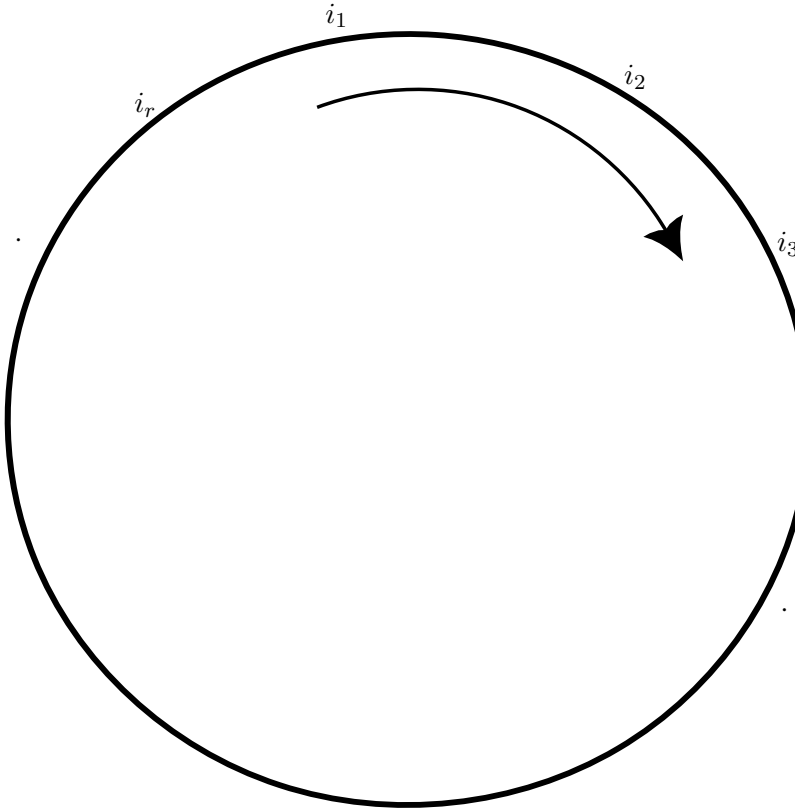


Figure 2: Cycle $\alpha = (i_1 \ i_2 \ \dots \ i_r)$.

We extend the cycle notation to 1-cycles, writing $(i) = (1)$ for all i , as a 1-cycle is the identity permutation: sending i to i and fixing the rest i.e. fixing everything.

There are r different cycle notations for any r -cycle α , since any i_j can be taken as its "starting point":

$$\alpha = (i_1 \ i_2 \ \dots \ i_r) = (i_2 \ i_3 \ \dots \ i_r \ i_1) = \dots = (i_r \ i_1 \ i_2 \ \dots \ i_{r-1}).$$

Definition 2.5

Two permutations $\alpha, \beta \in \mathfrak{S}_n$ are **disjoint** iff every i moved by one is fixed by the other: if $\alpha(i) \neq i$ then $\beta(i) = i$, and if $\beta(j) \neq j$ then $\alpha(j) = j$. A family $(\beta_k)_{k=1}^t$ of permutations is *disjoint* iff each pair of them is disjoint.

Example 2.5

Two cycles $(i_1 \dots i_r)$ and $(j_1 \dots j_s)$ are disjoint iff $(i_1 \dots i_r) \cap (j_1 \dots j_s) = \emptyset$.

Proposition 2.1

Disjoint permutations $\alpha, \beta \in S_n$ commute.

Proof. It suffices to prove that if $1 \leq i \leq n$, then $\alpha\beta(i) = \beta\alpha(i)$. If β moves i , say, $\beta(i) = j \neq i$, then β also moves j (as β is an injection $\beta(j) \neq \beta(i)$ when $i \neq j$); since α and β are disjoint, α must then fix i and j . So

$$\beta(\alpha(i)) = \beta(i) = j = \alpha(j) = \alpha(\beta(i))$$

$$\text{i.e. } \beta\alpha(i) = \alpha\beta(i).$$

The same conclusion holds if α moves i . Finally, if α and β both fix i , then $\alpha\beta(i) = i = \beta\alpha(i)$. \square

§2.3 Abstract groups and monoids

Definition 2.6 (Abstract group and monoid)

A **group** is a set G with a binary operation $G \times G \rightarrow G$ (usually written $(a, b) \mapsto a + b, a \times b, a \cdot b, a \circ b$, or just ab) such that

1. There is an **identity element** in G (denoted $e, 1$, or 0) such that $ea = a = ae$ for every a in G .
2. For every $a \in G$ there exists an **inverse element** $a^{-1} \in G$ such that $aa^{-1} = e = a^{-1}a$.
3. The operation is **associative**: $(ab)c = a(bc) \forall a, b, c \in G$.

If the operation is $(a, b) \mapsto a + b$, G is an additive group. If the operation is $(a, b) \mapsto ab$, G is a multiplicative group. By default, we write the operation the multiplicative way. If we do not require the second axiom (*existence of inverses*), then we have a **monoid**. If we do not require the first axiom (*existence of identity*) and second axiom, then we have a **semigroup**. If we only require closure, then we have a **groupoid** (or **magma**).

Axiom introduced	Algebraic structure
Closure	Groupoid (or magma)
Associativity	Semigroup
Identity	Monoid
Inverse	Group

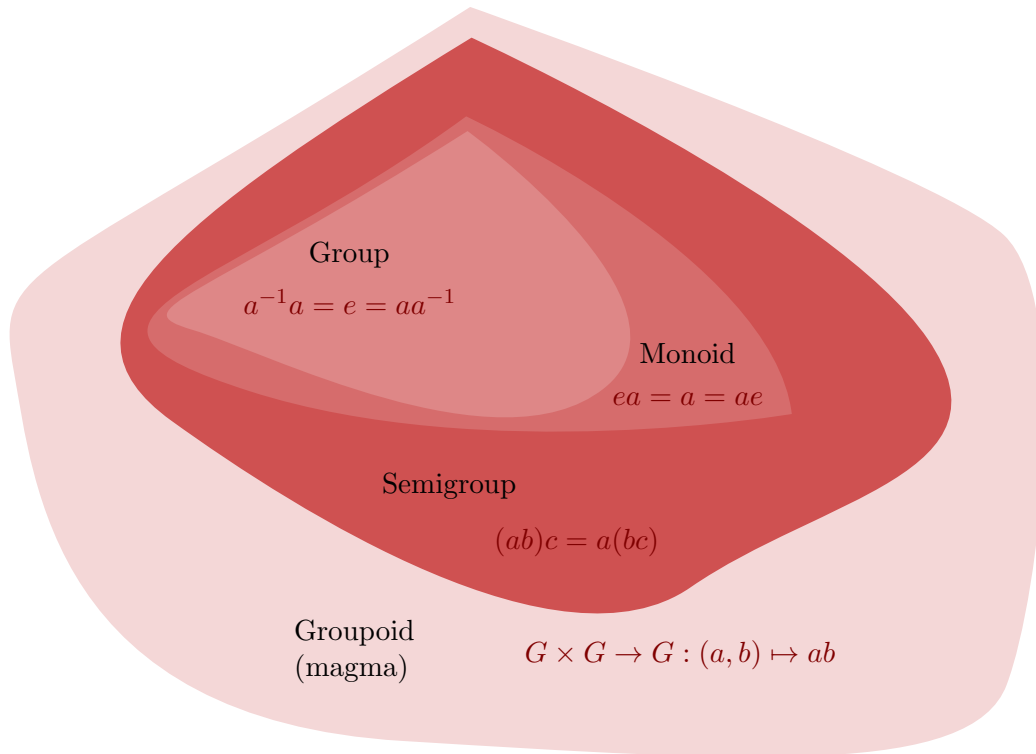


Figure 3: Some abstract algebraic structures

Remark. It is clear that if we take the composition of symmetries as our binary relation,

then the concrete notion of a group can be translated to the abstract notion. It is a subtle and important point that the converse is also true, which is what Cayley's Theorem says as we shall see in the next section.

Also, it is clear from the examples of the symmetries of a cube, the composition of permutations, subtraction of numbers and product of matrices (from linear algebra) why we want ordered pairs in the binary operation: as ab and ba can be different. Nevertheless, there are examples of groups where the commutative law $ab = ba$ holds, such as S_2 . In fact, Abel proved that if the Galois group of a polynomial is commutative, then f is solvable by radicals. As a result,

Definition 2.7

A group G is called **abelian** iff it satisfies the **commutative law**:

$$ab = ba$$

for every $a, b \in G$.

There are many examples of groups.

Example 2.6 1. The set S_X of all permutations of a set X , with composition as binary operation and $1_X = (1)$ as the identity, is a group, called the **symmetric group** on X . For a finite set X with $|X| = n$ the symmetric group is denoted as S_n . The groups S_n for $n \geq 3$ are nonabelian because $\begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 3 \end{pmatrix}$ do not commute:

$$\begin{pmatrix} 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}.$$

2. Consider $A, B, C \in M_n(\mathbb{F})$ (the set of square matrices of order n over the field \mathbb{F}) with addition operation $+$. Then $A + B \in M_n(\mathbb{F})$ so it is closed under addition. Also $A + (B + C) = (A + B) + C$ and $A + (-1)(A) = A - A = O$ where O is the $n \times n$ zero matrix and (-1) is the inverse of the identity element of \mathbb{F} . In fact we also have $A + B = B + A$. Thus, $(M_n(\mathbb{F}), +)$ is an abelian group.
3. Consider the same set as above, but with matrix product $\cdot : M_n(\mathbb{F}) \times M_n(\mathbb{F}) \rightarrow M_n(\mathbb{F})$, $(A, B) \mapsto P$ defined by

$$p_{ij} = \sum_{1 \leq k \leq n} a_{ik} b_{kj}.$$

So,

$$AB = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & b_{nn} \end{pmatrix}$$

$$\begin{aligned}
 &= \begin{pmatrix} (a_{11} \ \dots \ a_{1n}) \begin{pmatrix} b_{11} \\ \vdots \\ b_{n1} \end{pmatrix} & \dots & (a_{11} \ \dots \ a_{1n}) \begin{pmatrix} b_{1n} \\ \vdots \\ b_{nn} \end{pmatrix} \\ &\vdots & \ddots & \vdots \\ (a_{n1} \ \dots \ a_{nn}) \begin{pmatrix} b_{11} \\ \vdots \\ b_{n1} \end{pmatrix} & \dots & (a_{n1} \ \dots \ a_{nn}) \begin{pmatrix} b_{1n} \\ \vdots \\ b_{nn} \end{pmatrix} \end{pmatrix} \\
 &= \begin{pmatrix} p_{11} & \dots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \dots & p_{nn} \end{pmatrix}
 \end{aligned}$$

which is clearly in $M_n(\mathbb{F})$. However, it may so happen that $\det(A) = 0$, i.e., that A is **singular** \iff there is no $B \in M_n(\mathbb{F})$ such that $AB = I$ where I is the $n \times n$ identity matrix. So A may not be invertible, and this set therefore can't be a group under matrix product unless subjected to certain constraints as in the following examples.

4. For a field \mathbb{F} and positive integer n consider the set

$$\mathbf{GL}_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) : \overbrace{\det(A)}^{\text{nonsingular}} \neq 0\}$$

with the operation of matrix multiplication. If $A, B \in \mathbf{GL}_n(\mathbb{F})$ then A^{-1}, B^{-1} exist. Now, $(AB)^{-1} = B^{-1}A^{-1}$. Now

$$\det(B^{-1}A^{-1}) = \det(B^{-1}\det(A^{-1})) = \frac{1}{\det(A)\det(B)} \neq 0.$$

So AB is nonsingular, thus the operation is closed. Matrix product is associative, I is the identity, and every element, being nonsingular, has an inverse by definition. Thus, $\mathbf{GL}_n(\mathbb{F})$ forms a nonabelian group, called the **general linear group**.

Note that, $\mathbf{GL}_n(\mathbb{F})$ is not an additive group as clearly $\mathbf{0} \notin \mathbf{GL}_n(\mathbb{F})$, and, in fact, $\mathbf{GL}_n(\mathbb{F})$ is not even closed under $+$.

5. For a field \mathbb{F} and positive integer n the set

$$\mathbf{SL}_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) : \det(A) = 1\}$$

is also a nonabelian group called the **special linear group**.

Example 2.7

A field \mathbb{F} is a group under addition and $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is a group under multiplication.

Example 2.8

Let X be a set and let 2^X denote the power set of X . Define addition over 2^X to be the symmetric difference $A+B = (A \cup B) \setminus (A \cap B)$, and multiplication over 2^X to be

intersection $A \cap B$. The **Boolean group** $\mathcal{B}(X)$ is the additive group $(2^X, +)$, with \emptyset as the zero element and with every element being its own inverse. Also, $(2^X, \cap)$ is a semigroup.

Example 2.9

The set \mathbb{Z} of all integers is an additive abelian group under ordinary addition $(a, b) \mapsto a + b$, with identity 0 and $-n$ being the additive inverse of each $n \in \mathbb{Z}$. However, \mathbb{Z}^* is not a group under multiplication; aside from ± 1 none of the elements in \mathbb{Z}^* have a multiplicative inverse.

The situation changes when we consider the integers modulo m for some positive integer m .

Lemma 2.1

Let G be a group.

- (i) **Cancellation Law**: If either $xa = xb$ or $ax = bx$, then $a = b$.
- (ii) The identity element $e \in G$ is the unique element with $ea = a = ae$ for any $a \in G$.
- (iii) Every $a \in G$ has a unique inverse: there is only one element $a^{-1} \in G$ such that $aa^{-1} = e = a^{-1}a$.
- (iv) $(a^{-1})^{-1} = a$ for any $a \in G$.

Proof. (iii) Let $xa = e$, $xb = e$. Then $e = e \Rightarrow xa = xb \Rightarrow a(xa) = a(xb)$

$$\Rightarrow ae = (ax)b \Rightarrow a = (xa)b = eb = b.$$

□

Definition 2.8 (Submonoid and subgroup)

Let M be a monoid. A subset $S \subseteq M$ is a **submonoid** of M iff S contains e and S is closed under the binary operation of M restricted to S , i.e. $s_1s_2 \in S$ for all $s_1, s_2 \in S$.

Let G be a group. A subset $H \subseteq G$ is a **subgroup** of G iff H contains e and $a, b \in H \implies ab^{-1} \in H$.

§2.4 Isomorphism and Cayley's theorem

Theorem 2.1 (Cayley's Theorem)

Every group G is isomorphic to a subgroup of the symmetric group S_G .

§2.5 Subgroups and submonoids generated by a subset and cyclic groups

Remark. Given a subset S of a monoid M or a group G , we often need to consider the smallest submonoid of M or subgroup of G containing S .

Consider the simplest possible groups: those with a single generator.

Definition 2.9

Let G be a group. If $a \in G$ such that $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$, we say that G is a cyclic group with generator a .

Theorem 2.2

Any two cyclic groups of the same order (finite or infinite) are isomorphic.

Theorem 2.3

Any subgroup of a cyclic group $\langle a \rangle$ is cyclic.

§2.6 Orbits and cosets

Theorem 2.4 (Lagrange)

The order of a subgroup H of a finite group G is a factor of the order of G . More precisely, we have

$$|G| = |H|[G : H].$$

Corollary 2.1

If G is a finite group of order n , then $x^n = e$ for every $x \in G$.

§2.7 Congruences, quotient monoids and groups

Definition 2.10

A subgroup K of a group G is said to be **normal** if $g^{-1}kg \in K$ for every $g \in G$ and $k \in K$. We then write $K \trianglelefteq G$.

§2.8 Homomorphisms

Definition 2.11

If M and M' are monoids, then a map $\eta : M \rightarrow M'$ is called a **homomorphism** iff

$$\eta(ab) = \eta(a)\eta(b), \quad \eta(e) = e', \quad a, b \in M.$$

Remark. The second condition is redundant if M' is a group. For, if the first holds then $\eta(e) = \eta(e^2) = \eta(e)^2$ and multiplying by $\eta(e)^{-1}$ we obtain $e' = \eta(e)$.

§2.9 Exercises

Exercise 2.5. Show that $(\mathbb{Q}^+, \cdot) \cong (\mathbb{Z}[x], +)$.

Exercise 2.6. Show that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff \gcd(m, n) = 1$.

Exercise 2.7. Let G be an abelian subgroup of the symmetric group S_n and p_1, \dots, p_k be all prime divisors of $|G|$. Prove that $p_1 + \dots + p_k \leq n$.

§3 Rings

§3.1 Definition and elementary properties

Definition 3.1 (Ring)

A **ring** is a structure consisting of a non-vacuous set R together with two binary operations $+$, \cdot in R and two distinguished elements $0 \in R$ such that

1. $(R, +)$ is an abelian group.
2. (R, \cdot) is a semigroup.
3. The distributive laws

$$\text{a) } a(b + c) = ab + ac$$

$$\text{b) } (b + c)a = ba + ca$$

hold for all $a, b, c \in R$.

If $1 \in R$ (so that (R, \cdot) becomes a monoid), then R is a **ring with identity 1**. Moreover, if $ab = ba$ for any $a, b \in R$ we say that R is a **commutative ring**.

We call $u \in R$ **invertible** or **unit** iff there exists $v \in R$ such that $uv = vu = 1$.

Example 3.1 1. The **trivial ring** $R = \{0\}$.

2. The **ring of polynomials** $R[x]$ over a ring R defined as the set,

$$\{a_0x^n + a_1x^{n-1} + \cdots + a_{n-2}x^2 + a_{n-1}x + a_n : n \in \mathbb{Z}^+, a_i \in R, i = 0, 1, \dots, n\}.$$

3. The ordinary integers $(\mathbb{Z}, +, \cdot)$, the integers modulo m , i.e., $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ for $m \geq 0$, the **Gaussian integers** $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$.
4. Examples of rings without identity include the even integers $(2\mathbb{Z}, +, \cdot)$ or the integrable functions, where $f : [0, \infty) \rightarrow \mathbb{R}$ is integrable iff f is bounded and

$$\int_0^\infty |f(x)| \, dx = \lim_{t \rightarrow \infty} \int_0^t |f(x)| \, dx < \infty.$$

If f, g are integrable then so are their pointwise sum $f + g$ and pointwise product fg . The identity can only be the constant function $E(x) = 1$ for all $x \in [0, \infty)$. But then E is not integrable, so the ring of integrable functions does not contain an identity.

Definition 3.2

An element x of a ring R is **nilpotent** iff $x^2 = 0$.

Definition 3.3

A ring R is called a **Boolean ring** iff every element of R is **idempotent**, i.e.,

$$x^2 = x \, \forall x \in R.$$

Example 3.2

The power set 2^X of a set X is a *Boolean ring* $(2^X, +, \cap)$ where $(2^X, +) = \mathcal{B}(X)$ is the Boolean group defined with addition defined as the symmetric difference.

§3.2 Integral domains, division rings and fields**Definition 3.4** (Integral domain)

A commutative ring R with identity $1 \neq 0$ is called an **integral domain** (**ID**) iff R has no zero divisors.

Definition 3.5 (Division ring)

A **division ring** is a ring R with identity $1 \neq 0$ such that every nonzero element of R is a unit. In other words, division by nonzero elements is defined.

Definition 3.6 (Field)

A **field** is a *commutative division ring*.

Definition 3.7 (Characteristic)

The **characteristic** of a ring R is the least positive integer n such that $nr = 0$ for all $r \in R$.

§3.3 Subrings and subfields**Definition 3.8** (Subring)

Let R be a ring and $\emptyset \neq S \subseteq R$. Then S is a **subring** of R iff

$$a, b \in S \implies a - b, ab \in S.$$

Definition 3.9 (Subfield)

Let \mathbb{F} be a field and S be a subring of \mathbb{F} . Then S is a **subfield** of R iff

$$1_F \in S, a \in S \setminus \{0\} \implies a^{-1} \in S.$$

Definition 3.10 (Prime field)

A field with no proper subfields is called a **prime field**.

Theorem 3.1

Only prime fields are \mathbb{Z}_p ($p = 1$ or prime) and \mathbb{Q} .

§3.4 Exercises

Exercise 3.2. (Topics in Abstract Algebra pp. 335-338; the numbering may differ from the textbook.)

1. Which of the following algebraic structures $(R, +, \cdot)$ form a ring ?

a) $(\mathbb{Z}, +, \cdot)$ with $a \cdot b := \max(a, b)$ for $a, b \in \mathbb{Z}$.

b) $(\mathbb{Z}, +, \cdot)$ with $a \cdot b := |a|b$ for $a, b \in \mathbb{Z}$.

c) $(\mathbb{Z}[\sqrt{2}], +, \cdot)$, where,

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) := (a + c) + (b + d)\sqrt{2},$$

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) := (ac + 2bd) + (ad + bc)\sqrt{2},$$

for $a, b, c, d \in \mathbb{Z}$.

d) $(\mathbf{GL}_n(\mathbb{R}), +, \cdot)$ with the usual matrix addition and multiplication.

2. Prove that $(\mathbb{Z}, \oplus, \odot)$ is a commutative ring with identity if for all $m, n \in \mathbb{Z}$ we define $m \oplus n := m + n - 1$, $m \odot n := m + n - mn$.

3. Prove that $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ is a ring with $a \cdot b = \frac{1}{2}ab$. Is there an identity in R ?

4. If $R = \{a, b, c, d\}$ is a ring, where $(R, +)$ and (R, \cdot) are given by,

$+$	a	b	c	d	\cdot	a	b	c	d
a	a	b	c	d	a	a	a	a	a
b	b	a	d	c	b	a	b		
c	c	d	a	b	c	a		c	
d	d	c	b	a	d	a	b	c	

then complete the multiplication table of (R, \cdot) .

Is R commutative ? Does it have identity ? Prove that R satisfies $x^2 = x$ for all $x \in R$.

5. Let R be some subset of the set of all real-valued continuous functions on \mathbb{R} with

$$(f + g)(x) := f(x) + g(x), (f \cdot g)(x) = f(x)g(x).$$

Verify if R is a ring when R is :

a) the set of constant functions,

b) the set of integer-valued functions,

c) the set of even integer-valued functions,

d) the set of twice differentiable functions having second derivative zero at $x = 0$,

e) the set of infinitely differentiable functions having first k derivatives zero at $x = 0$.

6. Let R be a ring. If $a, b \in R$ then prove that $-(-a) = a$ and $-(a - b) = -a + b$.

7. Let R be a ring. If $a, b \in R$ and $m, n \in \mathbb{Z}$ then prove that

a) $n(ab) = (na)b = a(nb)$,

b) $(ma)(nb) = (mn)ab$,

- c) $n(-a) = (-n)a$.
8. Prove that a ring R is commutative iff $(a + b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$.
9. Prove that a ring R is commutative iff $(a + b)(a - b) = a^2 - b^2$ for all $a, b \in R$.
10. Give an example of a ring where:
- a) $(a + b)^2 \neq a^2 + 2ab + b^2$.
- b) $(a + b)(a - b) \neq a^2 - b^2$.
11. If R is a commutative ring with identity, show that for all $n \in \mathbb{Z}^+$
- $$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k.$$
12. Let $(R, +, \cdot)$ be a structure and assume all the conditions of a ring are satisfied by R except that we do not assume $(R, +)$ to be abelian. Suppose there is an element $c \in R$ such that $ca = cb \implies a = b$, i.e., c can be left cancelled, for any $a, b \in R$. Then show that $(R, +, \cdot)$ is a ring.
13. Show that the direct product of two commutative rings with identity is a commutative ring with identity.
14. If in a ring R we have $x^3 = x$ for all $x \in R$, then show that R is commutative.
15. Prove that every ring of order 15 is commutative.
16. Let $\mathbb{H} = \{a_0 + a_1i + a_2j + a_3k : a_r \in \mathbb{R}, r = 0, 1, 2, 3\}$ such that $a_0 + a_1i + a_2j + a_3k = b_0 + b_1i + b_2j + b_3k \iff a_r = b_r$ for $r = 0, 1, 2, 3$. Define addition and multiplication as a formal sum and product using the relations:
- $$i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j.$$
- Prove that \mathbb{H} is a noncommutative ring with identity (**the ring of real quaternions**).
17. Prove that a ring R with identity is a Boolean ring iff $a(a + b)b = 0$ for all $a, b \in R$.
18. Suppose $m, n \in \mathbb{Z}^+ : m, n > 1$ and $\gcd(m, n) = 1$. Prove that \mathbb{Z}_{mn} has at least four idempotent elements.
19. Find all idempotent elements of the rings \mathbb{Z}_6 , \mathbb{Z}_8 and \mathbb{Z}_{12} .
20. Find all positive integers n for which the only idempotents of \mathbb{Z}_n are $[0]$ and $[1]$.
21. In a ring R with identity, show that
- a) $a(-1) = (-1)a = -a$ for all $a \in R$,
- b) if a is a unit in R then $-a$ is also a unit in R and $(-a)^{-1} = -a^{-1}$,
- c) if $ab + ba = 1_R$ and $a^3 = a$, then $a^2 = 1_R$.
22. Find the group of units in each of the rings: \mathbb{Z}_7 , \mathbb{Z}_{12} , \mathbb{Z}_n ; find all units of $M_2(\mathbb{Z})$; prove that $\mathbb{Z}[x]$ and \mathbb{Z} have the same units.
23. In a finite ring with identity show that $ab = 1 \implies ba = 1$. Hence prove that a finite ring with prime number of elements is commutative.

24. In a ring R if there exists a unique $a \in R$ such that $xa = x$ for all $x \in R$, prove that $ax = x$.
25. In a ring with identity if $a^2 = a$ then show that $1 - 2a$ is a unit.
26. Show that the units of $\mathbb{R}[x]$ are nonzero constant polynomials.
27. Let R be a ring such that $1 - ab$ is a unit for some $a, b \in R$. Then show that $1 - ba$ is also a unit and $(1 - ba)^{-1} = 1 + b(1 - ab)^{-1}a$.

Answer. (The numbering may differ from the textbook.)

1. a) $a \cdot (b + c) = \max(a, b + c)$ and $ab + ac = \max(a, b) + \max(a, c)$. If we pick $c < a < b$, then,

$$\max(a, b + c) = b + c \neq b + a = \max(a, b) + \max(a, c).$$

For example, let $a = 2, b = 3, c = 1$. Then

$$2(3 + 1) = \max(2, 3 + 1) = 4 \neq 5 = \max(2, 3) + \max(2, 1).$$

So not a ring.

- b) $(b + c)a = |b + c|a$ and $ba + ca = (|b| + |c|)a$. But by triangle inequality, $|b + c| \leq |b| + |c|$, so that $(b + c)a \neq ba + ca$ in general. So not a ring.
- c) Clearly $\mathbb{Z}[\sqrt{2}]$ is closed under $+$ and \cdot . $+$ is associative and commutative as ordinary addition is associative and commutative, and \cdot is associative as:

$$\begin{aligned} (x + y\sqrt{2})((a + b\sqrt{2})(c + d\sqrt{2})) &= (xac + 2ybd) + (xad + ybc)\sqrt{2} \\ &= ((x + y\sqrt{2})(a + b\sqrt{2}))(c + d\sqrt{2}). \end{aligned}$$

$0 = 0 + 0\sqrt{2}$ and for every $a + b\sqrt{2}$ there is an element $-a - b\sqrt{2}$ such that

$$(a + b)\sqrt{2} + (-a - b)\sqrt{2} = 0,$$

so $(\mathbb{Z}[\sqrt{2}], +)$ is an abelian group. Also $(\mathbb{Z}[\sqrt{2}], \cdot)$ is a semigroup, so we need to just verify the two distributive laws,

$$\begin{aligned} (x + y\sqrt{2})(a + b\sqrt{2} + c + d\sqrt{2}) &= (x + y\sqrt{2})((a + c) + (b + d)\sqrt{2}) \\ &= (x(a + c) + 2y(b + d)) + (x(b + d) + y(a + c))\sqrt{2} \\ &= (xa + 2yb) + (xb + ya)\sqrt{2} + (xc + 2yd) + (xd + yc)\sqrt{2} \\ &= (x + y\sqrt{2})(a + b\sqrt{2}) + (x + y\sqrt{2})(c + d\sqrt{2}), \\ (a + b\sqrt{2} + c + d\sqrt{2})(x + y\sqrt{2}) &= ((a + c) + (b + d)\sqrt{2})(x + y\sqrt{2}) \\ &= ((a + c)x + 2(b + d)y) + ((b + d)x + (a + c)y)\sqrt{2} \\ &= (ax + 2by) + (bx + ay)\sqrt{2} + (cx + 2dy) + (dx + cy)\sqrt{2} \\ &= (a + b\sqrt{2})(x + y\sqrt{2}) + (c + d\sqrt{2})(x + y\sqrt{2}). \end{aligned}$$

Thus, $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ is a ring.

- d) $\mathbf{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$ so clearly $\mathbf{0} \notin \mathbf{GL}_n(\mathbb{R})$.

Thus, $(\mathbf{GL}_n(\mathbb{R}), +, \cdot)$ is not a ring.

2. Let $m, n \in \mathbb{Z}$, then $m \oplus n, m \odot n \in \mathbb{Z}$. Also $m \oplus n = m + n - 1 = n + m - 1 = n \oplus m$. Let $\ell \in \mathbb{Z}$. Then

$$\ell \oplus (m \oplus n) = \ell \oplus (m + n - 1) = \ell + (m + n - 1) - 1 = (\ell + m - 1) + n - 1 = (\ell \oplus m) \oplus n.$$

Also

$$1 \oplus m = m \oplus 1 = m, \quad m \oplus (2 - m) = (2 - m) \oplus m = 1$$

so (\mathbb{Z}, \oplus) is an additive abelian group. Now,

$$\ell \odot (m \odot n) = \ell + m + n - \ell mn = (\ell \odot m) \odot n$$

so (\mathbb{Z}, \odot) is a semigroup. Furthermore, $m \odot n = m + n - mn = n + m - nm = n \odot m$ so it is commutative. As \oplus and \odot are commutative, we need to verify only one of the distributive laws,

$$\begin{aligned} & \ell \odot (m \oplus n) \\ &= \ell \odot (m + n - 1) = 2\ell + m + n - \ell m - \ell n - 1 = (\ell + m - \ell m) \oplus (\ell + n - \ell n) \\ &= (\ell \odot m) \oplus (\ell \odot n). \end{aligned}$$

Now, $0 \odot m = m \odot 0 = m$, so $(\mathbb{Z}, \oplus, \odot)$ is a commutative ring with identity 0.

3. $(\mathbb{Z}/2\mathbb{Z}, +)$ is an additive abelian group. If $a, b \in \mathbb{Z}/2\mathbb{Z}$ then $a = 2m, b = 2n$ for some $m, n \in \mathbb{Z}$. So,

$$a \cdot b = \frac{1}{2} 4^2 mn = 2mn \in \mathbb{Z}/2\mathbb{Z}.$$

As ordinary multiplication is commutative and associative, \cdot is also commutative and associative. Thus $(\mathbb{Z}/2\mathbb{Z}, \cdot)$ is a semigroup and we only need to check one of the distributive laws

$$a \cdot (b + c) = \frac{a}{2}(b + c) = \frac{ab}{2} + \frac{ac}{2} = a \cdot b + a \cdot c.$$

Also, $2 \cdot m = m = m \cdot 2$. Thus, $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ is a (commutative) ring with identity 2.

4. From the given tables, $d^2 = d(b + c) = db + dc = b + c = d$, $cb = (b + d)b = b^2 + db = b + b = a$, $bc = a$, $bd = (d + c)d = d^2 + cd = d + c = b$, $bc = b(b + d) = b^2 + bd = b + b = a$, and $c^2 = c(b + d) = cb + cd = a + c = c$. Thus the multiplication table for R is:

\cdot	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	a	c	c
d	a	b	c	d

As the table is symmetric along its diagonal, R is a commutative ring. From the above table clearly $x^2 = x$ for $x \in R$, and d is the identity as $xd = dx = x$.

5. a) If $R = \{f : \mathbb{R} \xrightarrow{\text{cont.}} \mathbb{R} \mid f(x) = c, c \in \mathbb{R}\}$, then the map $\phi(f) = f(x_0)$ for some $x_0 \in \mathbb{R}$ defines an isomorphism from R to \mathbb{R} , i.e., $(R, +, \cdot) \cong (\mathbb{R}, +, \cdot)$ which is a ring.
- b) Let $R = \{f : \mathbb{R} \xrightarrow{\text{cont.}} \mathbb{Z}\}$, but if $f : \mathbb{R} \rightarrow \mathbb{Z}$ is continuous then f must be constant. Thus, similar to the previous case, there exists the isomorphism $\phi : R \rightarrow \mathbb{Z}$ such that $\phi(f) = f(x_0)$ for some $x_0 \in \mathbb{R}$, i.e., $(R, +, \cdot) \cong (\mathbb{Z}, +, \cdot)$ which is a ring.

- c) Similar to the previous case, we define an isomorphism $\phi : R \rightarrow 2\mathbb{Z}$ such that $\phi(f) = f(x_0)$ for some $x_0 \in \mathbb{R}$, i.e., $(R, +, \cdot) \cong (2\mathbb{Z}, +, \cdot)$ which is a ring.
- d) Consider $f(x) = x$, and $g(x) = -x$ in R . Then the function $(f \cdot g)(x) = -x^2$ is continuous and twice-differentiable but $(f \cdot g)''(0) = -2 \neq 0$ so R is not closed under pointwise multiplication.
- e) In this case, $f \cdot g$ is in R as the first k derivatives all vanish at $x = 0$. So for all $j \leq k$ we have $f^{(j)} = g^{(j)} = 0$, implying $(f \cdot g)^{(k)} \neq 0$ for any $k \in \mathbb{Z}^+$. So R is closed under pointwise multiplication. The values of the functions in R are all real, so by the properties of the real numbers the functions in R are commutative, associative and distributive by virtue of \mathbb{R} being a ring. So R is a ring.
6. $a \in R \implies \exists(-a) \in R : a + (-a) = 0 = (-a) + (-(-a))$

$$\xRightarrow{\text{subtract } (-a)} a = -(-a).$$

Similarly,

$$(a - b) + (-a + b) = 0 = (a - b) + (-(a - b)) \implies (-(a - b)) = -a + b.$$

7. $n(ab) = \underbrace{(ab + \cdots + ab)}_{n \text{ times}} = \underbrace{(a + \cdots + a)}_{n \text{ times}} b = (na)b = a \underbrace{(b + \cdots + b)}_{n \text{ times}} = a(nb)$. Similarly,

$$\begin{aligned} (ma)(nb) &= \underbrace{(a + \cdots + a)}_{m \text{ times}} (nb) = \underbrace{(a(nb) + \cdots + a(nb))}_{m \text{ times}} \\ &= \underbrace{((\underbrace{ab + \cdots + ab}_{n \text{ times}})) + \cdots + ((\underbrace{ab + \cdots + ab}_{n \text{ times}}))}_{m \text{ times}} \\ &= \underbrace{(ab + \cdots + ab)}_{mn \text{ times}} = mn(ab). \end{aligned}$$

Also,

$$n(-a) = n(1)(-a) = n(-1)a = (-n)a.$$

8. Given: $(a+b)^2 = a^2 + 2ab + b^2$. In general, in a ring $(a+b)^2 = a(a+b) + b(a+b) = a^2 + ab + ba + b^2$. So

$$\begin{aligned} (a+b)^2 &= (a+b)^2 \\ \implies a^2 + 2ab + b^2 &= a^2 + ab + ba + b^2 \\ \implies ab + ab &= ab + ba \implies ab = ba. \end{aligned}$$

9. Given: $(a+b)(a-b) = a^2 - b^2$. In general, in a ring $(a+b)(a-b) = a(a-b) + b(a-b) = a^2 - ab + ba - b^2$. So

$$\begin{aligned} (a+b)(a-b) &= (a+b)(a-b) \\ \implies a^2 - b^2 &= a^2 - ab + ba - b^2 \\ \implies 0 &= -ab + ba \implies ab = ba. \end{aligned}$$

10. Matrix multiplication is noncommutative. So, for example, in the ring of 2×2 real matrices $M_2(\mathbb{R})$,

$$(A + B)^2 \neq A^2 + 2AB + B^2, \quad (A + B)(A - B) \neq A^2 - B^2.$$

11. The base cases

$$\begin{aligned} (a + b)^1 &= \binom{1}{0} a^{1-0} b^0 + \binom{1}{1} a^{1-1} b^1 = a + b, \\ (a + b)^2 &= \binom{2}{0} a^2 + \binom{2}{1} ab + \binom{2}{2} b^2 = a^2 + 2ab + b^2, \end{aligned}$$

hold as R is commutative. Now assume that for some $n \in \mathbb{Z}^+$ the hypothesis $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$ holds. Then,

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n = (a + b) \left(\sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \right) \\ &= (a + b) \left(a^n + \sum_{k=1}^{n-1} \binom{n}{k} a^{n-k} b^k + b^n \right) \\ &= a^{n+1} + a^n b + \sum_{k=1}^{n-1} \binom{n}{k} (a + b) a^{n-k} b^k + ab^n + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n-1} \binom{n}{k} a^{n+1-k} b^k + ab^n + a^n b + \sum_{k=1}^{n-1} \binom{n}{k} a^{n-k} b^{k+1} + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^n \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^{k+1} + b^{n+1} \\ &= a^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=1}^n \binom{n}{k-1} a^{n+1-k} b^k + b^{n+1} \\ &= \binom{n+1}{0} a^{n+1} + \sum_{k=1}^n \left(\binom{n}{k} + \binom{n}{k-1} \right) a^{n+1-k} b^k + \binom{n+1}{n+1} b^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k = (a + b)^{n+1}. \end{aligned}$$

Thus, proved by induction on n .

- 12.

$$\begin{aligned} (c + c)(a + b) &= c(a + b) + c(a + b) = \cancel{ca} + cb + ca + \cancel{cb}, \\ (c + c)(a + b) &= (c + c)a + (c + c)b = \cancel{ca} + ca + cb + \cancel{cb}, \\ \implies cb + ca &= ca + cb \implies c(b + a) = c(a + b) \implies b + a = a + b. \end{aligned}$$

Thus $(R, +)$ is an abelian group so R is a ring.

13. Let R and S be commutative rings. $R \times S$ is an additive abelian group under componentwise addition. Now, if $r_i \in R$, $s_i \in S$ then

$$(r_1, s_1)((r_2, s_2)(r_3, s_3)) = (r_1, s_1)(r_2 r_3, s_2 s_3)$$

$$\begin{aligned}
 &= (r_1(r_2r_3), s_1(s_2s_3)) \\
 &= ((r_1r_2)r_3, (s_1s_2)s_3) \\
 &= (r_1r_2, s_1s_2)(r_3, s_3) \\
 &= ((r_1, s_1)(r_2, s_2))(r_3, s_3).
 \end{aligned}$$

So componentwise multiplication is associative, making $R \times S$ a semigroup under this operation. Also as R, S are commutative we have

$$(r_1, s_1)(r_2, s_2) = (r_1r_2, s_1s_2) = (r_2r_1, s_2s_1) = (r_2, s_2)(r_1, s_1),$$

so $R \times S$ is commutative. Thus we need only check one distributive law:

$$\begin{aligned}
 (r_1, s_1)((r_2, s_2) + (r_3, s_3)) &= (r_1, s_1)(r_2 + r_3, s_2 + s_3) \\
 &= (r_1(r_2 + r_3), s_1(s_2 + s_3)) \\
 &= (r_1r_2 + r_1r_3, s_1s_2 + s_1s_3) \\
 &= (r_1r_2, s_1s_2) + (r_1r_3, s_1s_3) \\
 &= (r_1, s_1)(r_2, s_2) + (r_1, s_1)(r_3, s_3).
 \end{aligned}$$

Furthermore, R and S are rings with identity so $(1, 1) \in R \times S$ and

$$(1, 1)(r, s) = (r, s) = (r, s)(1, 1).$$

So $R \times S$ is a commutative ring with identity.

14. $o(R) = |R| = 15$ and $(R, +)$ is an abelian group. Thus by Cauchy's Theorem on Finite Abelian Groups we have

$$\begin{cases} 3 \mid o(R) \implies \exists a \in R : o(a) = 3, \\ 5 \mid o(R) \implies \exists b \in R : o(b) = 5 \end{cases}, \quad ab = ba, \quad \gcd(o(a), o(b)) = 1,$$

thus $o(ab) = o(a)o(b) = 15$ and R is cyclic under addition i.e. $R = \langle c \rangle = \{nc : n \in \mathbb{Z}\}$ and clearly

$$\overset{x}{n_1}\overset{y}{c} \cdot \overset{y}{n_2}\overset{x}{c} = \overset{y}{n_2}\overset{x}{c} \cdot \overset{x}{n_1}\overset{y}{c}.$$

15. Given $x^3 = x$ for all $x \in R$. Thus, $ab = 0 \implies ba = (ba)^3 = b(ab)(ab)a = 0$.
The center of the ring R is $Z(R) = \{c \in R : cx = xc \forall x \in R\}$.
Then, $c^2 = c \implies c \in Z(R)$ because

$$\begin{cases} cx = c^2x \implies c(x - cx) = 0 \implies (x - cx)c = 0 \implies xc = cxc, \\ xc = xc^2 \implies (x - xc)c = 0 \implies c(x - xc) = 0 \implies cx = cxc. \end{cases}$$

Now, for all $x \in R : x^3 = x \implies x^4 = x^2 \implies x^2 \in Z(R)$.

Also, $c^2 = 2c \implies c \in Z(R)$ as $c = c^3 = 2c^2 = c^2 + c^2$ and $c^2 \in Z(R)$. Now,

$$(x + x^2)^2 = (x + x^2)(x + x^2) = x^2 + x^3 + x^3 + x^4 = x^2 + x + x + x^2 = 2(x + x^2),$$

so $(x + x^2) \in Z(R)$. Thus, for any $x \in R$

$$x + x^2, x^2 \in R \implies x = (x + x^2) - x^2 \in R.$$

Thus R is commutative.

16. We define addition in the real quaternions as

$$\begin{aligned} & (a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}) + (b_0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}) \\ &= (a_0 + b_0) + (a_1 + b_1)\mathbf{i} + (a_2 + b_2)\mathbf{j} + (a_3 + b_3)\mathbf{k}. \end{aligned}$$

Then as real numbers are an additive abelian group, \mathbb{H} is also an additive abelian group under this componentwise addition.

The elements $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ can be defined in matrix form as

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

then the matrix form of $(a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k})$ is

$$\begin{pmatrix} a_0 + a_1i & a_2 + a_3i \\ -a_2 + a_3i & a_0 - a_1i \end{pmatrix}.$$

Then we can define the product of two quaternions to be the matrix multiplication of their matrix forms,

$$\begin{pmatrix} a_0 + a_1i & a_2 + a_3i \\ -a_2 + a_3i & a_0 - a_1i \end{pmatrix} \begin{pmatrix} b_0 + b_1i & b_2 + b_3i \\ -b_2 + b_3i & b_0 - b_1i \end{pmatrix}.$$

Thus by associativity and distributivity of matrix multiplication, we have associativity and distributivity of quaternion multiplication. But matrix multiplication is noncommutative in general, so quaternion multiplication is noncommutative in general.

Thus \mathbb{H} is a noncommutative ring with identity $\mathbf{1}$.

17. $a(a+b)b = a^2b + ab^2 = ab + ab = 2ab$ by property of Boolean ring. Now suppose

$$\begin{aligned} a(a+b)b = 0 & \implies a^2b + ab^2 = 0 \\ & \xrightarrow{\text{set } b=-1} -a^2 + a = 0 \implies a = a^2 \end{aligned}$$

so it is a Boolean ring.

18. By Chinese Remainder Theorem, if $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, then

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}.$$

Thus, $\mathbb{Z}/mn\mathbb{Z} \cong \underbrace{\mathbb{Z}/m\mathbb{Z}}_{[0]_m, [1]_m} \times \underbrace{\mathbb{Z}/n\mathbb{Z}}_{[0]_n, [1]_n}$. So there are at least four idempotents in R of the form,

$$(0, 0), (0, 1), (1, 0), (1, 1).$$

19. $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ so the idempotents are $[0]$ (congruent to 0 mod 2 and 3), $[1]$ (congruent to 1 mod 2 and 3), $[3]$ (congruent to 1 mod 2 and 0 mod 3), $[4]$ (congruent to 0 mod 2 and 1 mod 3). The idempotents in \mathbb{Z}_8 are only $[0]$ and $[1]$ as 8 has no prime factors other than 2.

$\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ so the idempotents are $[0]$ (congruent to 0 mod 4 and 3), $[1]$ (congruent to 1 mod 4 and 3), $[4]$ (congruent to 0 mod 4 and 1 mod 3), $[9]$ (congruent to 1 mod 4 and 0 mod 3).

20. **(Problem 21 in the textbook)** If the only idempotents \mathbb{Z}_n in are $[0]$ and $[1]$ then $n = p^k$ for some prime p and $k \in \mathbb{Z}^+$.

21. **(Problem 23 in the textbook)** In a ring R with identity,

a)

$$\begin{aligned} a(-1) + a(1) &= a(-1 + 1) = a0 = 0 \implies a(-1) = -a \\ (-1)a + (1)a &= (-1 + 1)a = 0a = 0 \implies (-1)a = -a \\ \therefore a(-1) &= (-1)a = -a. \end{aligned}$$

b) a is a unit so $ar = ra = 1$ for some $r \in R$. Then

$$\begin{aligned} -ar &= -ra = -1 \\ \implies (-a)(-r) &= (-r)(-a) = 1 \\ \implies -r &= -a^{-1} \implies -(a)^{-1} = -a^{-1}. \end{aligned}$$

c) Given $a^3 = a$, $ab + ba = 1_R$. Then,

$$\begin{aligned} a^2(ab + ba) &= a^2 \implies a^3b + a^2ba = a^2 \implies ab + aaba = a^2 \\ &\implies ab + a(1_R - ba)a = a^2 \\ &\implies ab + a^2 - aba^2 = a^2 \\ &\implies ab(1_R - a^2) = 0. \end{aligned}$$

Similarly, $(ab + ba)a^2 = a^2 \implies (1_R - a^2)ba = 0$.

$$\begin{aligned} &\implies ab(1_R - a^2) + (1_R - a^2)ba = 0 \\ \implies ab - aba^2 + ba - a^2ba &= ab + ba - a(ab + ba)a = 0 \\ &\implies 1_R - a^2 = 0 \implies a^2 = 1_R. \end{aligned}$$

22. **(Problem 24 in the textbook)** The units of \mathbb{Z}_n are $\{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}$, so units of \mathbb{Z}_7 are $\{[1], \dots, [6]\}$ and units of \mathbb{Z}_{12} are $\{[1], [5], [7], [11]\}$.

If $A \in M_2(\mathbb{Z})$ then $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible iff $\det(A) \neq 0$, then

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

which has integer entries iff $\det(A) = \pm 1$. So the units of $M_2(\mathbb{Z})$ are $\{A \in M_2(\mathbb{Z}) : \det(A) = \pm 1\}$.

If $fg = 1$ in $\mathbb{Z}[x]$ then fg is a nonzero constant polynomial, so f, g must be nonzero constant polynomials, so there must exist nonzero integers $a, b \in \mathbb{Z} : f = a, g = b$ with $ab = \pm 1$. So the units of $\mathbb{Z}[x]$ are $\{-1, +1\}$ which is the same as the units of \mathbb{Z} .

23. **(Problem 26 (a) in the textbook)** $ab = 1$. Let $R = \{a_1, \dots, a_n\}$, $S = \{ba_1, \dots, ba_n\}$. Then,

$$ba_i = ba_j \implies aba_i = aba_j \implies a_i = a_j$$

thus $|S| = |R|$ but $S \subseteq R$ so $S = R$. Now,

$$ba_i = 1 \implies aba_i = a \implies a_i = a.$$

Thus, $ba = 1$.

(Problem 26 (c) in the textbook) If $o(R) = p$ prime then due to R being an additive abelian group we have by Cauchy's Theorem on Finite Abelian Groups that R is cyclic and generated by 1. Thus, R is commutative.

24. **(Problem 27 in the textbook)** Let $r \in R$ be arbitrary. Then $x(ar - r + a) = xar - xr + xa = x$ for all $x \in R$. But a is unique, so $ar - r + a = a \implies ar = r$. As r was arbitrary we are done.

25. **(Problem 28 in the textbook)** Required to show: $x(1 - 2a) = (1 - 2a)x = 1$.

$$(1 - 2a)^2 = 1 - 4a + 4a^2 = 1 \text{ as } a^2 = a$$

thus $(1 - 2a) = 1$, and in a Boolean ring, $x1 = 1x = 1$.

26. **(Problem 29 in the textbook)** Let $fg = 1 \implies fg$ is a constant (nonzero) polynomial i.e. of degree 0. Then, $\deg(f)\deg(g) \leq 0$ so that f, g are constant nonzero polynomials. Thus the units of $\mathbb{R}[x]$ is the ring of constant nonzero polynomials
27. **(Problem 32 in the textbook)** Let $c = (1 - ab)^{-1}$. Then expanding as a geometric series,

$$\begin{aligned} (1 - ba)^{-1} &= 1 + ba + baba + bababa + \dots \\ &= 1 + b(1 + ab + abab + \dots)a \\ &= 1 + bca. \end{aligned}$$

Verifying,

$$\begin{aligned} (1 - ba)(1 + bca) &= 1 - ba + bca - babca \\ &= 1 - ba + b(c - abc)a = 1 - ba + b(1 - ab)ca \\ &= 1 - ba + ba = 1. \end{aligned}$$

So indeed $(1 - ba)^{-1} = 1 + bca = 1 + b(1 - ab)^{-1}a$.