Algebra

Sayan Das (dassayan0013@gmail.com)

June 30, 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

§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

$$|z| > M \implies |P(z)| \geq |a_n| \tag{1}$$

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

$$|z| \leq M \implies |P(z)| \geq |P(z_0)|\,. \tag{2}$$

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

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

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 $Q \in \mathbb{C}[z]$,

$$P(z) = Q(z - z_0). \tag{4}$$

By (3) and (4),

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

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

$$Q(z) = c_n + c_{n-k}z^k + \sum_{j=k+1}^{n} c_{n-j}z^j \quad (c_{n-k} \neq 0)$$

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

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

$$c_{n-k}z_1^k = -c_n. \tag{7}$$

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

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

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 $0 < \varepsilon < 1$,

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

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

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 $Q(0) = c_n = 0$. □

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 $k = 2, \ldots, n$ 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 $f(x) = (x - \alpha_1)f_1(x)$

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

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

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

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

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

Theorem 1.3 (Complex conjugate root theorem)
If $f \in \mathbb{R}[x] : f(\zeta) = 0$ for some $\zeta \in \mathbb{C}$, then $f(\overline{\zeta}) = 0$.

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

$$\implies \sum_{j=0}^{n} a_{n-j}\zeta^j = 0$$

$$\implies \overline{\sum_{j=0}^{n} a_{n-j}\zeta^j} = \overline{0}$$

$$\implies \sum_{j=0}^{n} \overline{a_{n-j}\zeta^j} = 0$$

$$\implies \sum_{j=0}^{n} a_{n-j}\overline{\zeta^j} = 0$$

$$\implies \sum_{j=0}^{n} a_{n-j}\overline{\zeta}^j = f(\overline{\zeta}) = 0.$$

Thus, $f(\overline{\zeta}) = 0$. □

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

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

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

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

with

$$\sigma_k = \sum_{1 \le i_1 < \cdots < i_k \le n} \left(\prod_{1 \le i \le k} \alpha_i \right)$$

in general, then:

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

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

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

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

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

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

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

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:

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

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

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 $(\operatorname{sgn}(a_j))_{j=0}^{n}$ 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

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

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:

$$ax^2+bx+c = a(x+bH)^2 - ab^2H^2 + c$$

$$\implies ax^2+bx+c = ax^2+2abHx+ab^2H^2-(ab^2H^2-c)$$

$$\therefore H = \frac{1}{2a},\ a(x+\frac{b}{2a})^2 - \frac{b^2-4ac}{4a} = 0$$

and consequently

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

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:

$$F\left(x - \frac{b}{3a}\right) = f(x) = ax^3 + \frac{(3ac-b^2)}{3a}x + \frac{2b^3-9abc+27a^2d}{27a^2}$$

$$= x^3 + \underbrace{\frac{(3ac-b^2)}{3a^2}}_{q} x + \underbrace{\frac{2b^3-9abc+27a^2d}{27a^3}}_{r}$$

$$= x^3 + qx + r$$

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

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

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

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

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 $R<0$)

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

□

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 $x=6,\quad 5\omega+\omega^2=-3+2i\sqrt{3},\quad 5\omega^2+\omega=-3-2i\sqrt{3}.$

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

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

then $g+h=\sqrt[3]{\frac{1}{2}\left(-6+i\frac{20\sqrt{3}}{9}\right)}+\sqrt[3]{\frac{1}{2}\left(-6-i\frac{20\sqrt{3}}{9}\right)}$

$$=\sqrt[3]{\left(-3+i\frac{10\sqrt{3}}{9}\right)}+\sqrt[3]{\left(-3-i\frac{10\sqrt{3}}{9}\right)}$$

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

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

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 $F\left(u - \frac{1}{4}b\right) = 0$. 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,

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

and determine j, ℓ, m (the linear terms have coefficients j and $-j$ as $f(x)$ has no cubic term). Expanding and equating like coefficients yields,

$$\begin{cases} \ell + m - j^2 = q, \\ j(m - \ell) = r, \\ \ell m = s. \end{cases}$$

The first two equations give,

$$\begin{cases} 2m = j^2 + q + r/j, \\ 2\ell = j^2 + q - r/j. \end{cases}$$

Substuting these values for m and ℓ into the third equation yields a cubic in j^2, called the **resolvent cubic**:

$$(j^2)^3 + 2q(j^2)^2 + (q^2 - 4s)j^2 - r^2.$$

The cubic formula gives j^2, from which we can determine m and ℓ and hence the roots of the quartic.

§1.1.6 Exercises

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

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

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

§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 $a_1, \ldots, a_n$ are arbitrary elements of $\mathbb{R}$, then

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

Theorem 1.10 (Weighted Arithmetic Mean $\geq$ Geometric Mean)

If $a_1, \ldots, a_n$ are arbitrary elements of $\mathbb{R}$ and $w_1, \ldots, w_n$ are nonnegative weights *with $w = w_1 + \cdots + w_n$, then*

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

Theorem 1.11 (Cauchy-Schwarz Inequality)
If $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ 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 $j = 1, \ldots, n$.

Theorem 1.12 (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 $f : D_f \to \mathbb{R}, D_f \subseteq \mathbb{R}$ *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 1.13 (Jensen's Inequality)
Let $f : D_f \to \mathbb{R}, D_f \subseteq \mathbb{R}$ and $\{x_j\}_{j=1}^n \subseteq D_f$ with $a_1, \ldots, a_n$ 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 1.14 (Minkowski's Inequality)

If $p \geq 1$ and $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ 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 1.15 (Hölder's Inequality)

If $p, q \geq 1 : 1/p + 1/q = 1$ and $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ 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 1.16 (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 1.17 (Rearrangement Inequality)

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

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

Theorem 1.18 (Weierstrass's Inequalities)

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

§2.1 Definitions and motivation

Remark. We first abstract the notion of a linear map and the kernel of a linear map from linear algebra.

Definition 2.1 (Homomorphism)

A **homomorphism** is a map $f : A \to B$ between two algebraic structures $(A, \star)$ and $(B, \circ)$ such that

$$a, b \in A \implies f(a \star b) = f(a) \circ f(b) \in B.$$

The **kernel** of a homomorphism f is

$$\ker f = \{a \in A : f(a) = e'\} = f^{-1}(\{e'\}),$$

where e' is the identity element of B.

A homomorphism is called a **monomorphism** if it is injective, **epimorphism** if it is surjective, **isomorphism** if it is bijective, **endomorphism** if $(A, \star) = (B, \circ)$, and **automorphism** if it is an endomorphism as well as isomorphism.

Condition introduced	Mapping type
$f(a \star b) = f(a) \circ f(b)$	Homomorphism
$f(a) = f(b) \implies a = b$	Monomorphism
$f(A) = B$	Epimorphism
$f : A \longleftrightarrow B$	Isomorphism
$A = B$	Endomorphism
$A = B \ \ \& \ f : A \longleftrightarrow B$	Automorphism

Remark. In the definition of a homomorphism, we additionally want $f(e) = e'$ (identity of A mapped to that of B). However, this condition is redundant for groups. In linear algebra we were mostly concerned with linear systems of the form

$$Ax = B.$$

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 2.2 (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.

We now consider some geometric examples of concrete groups.

Example 2.1

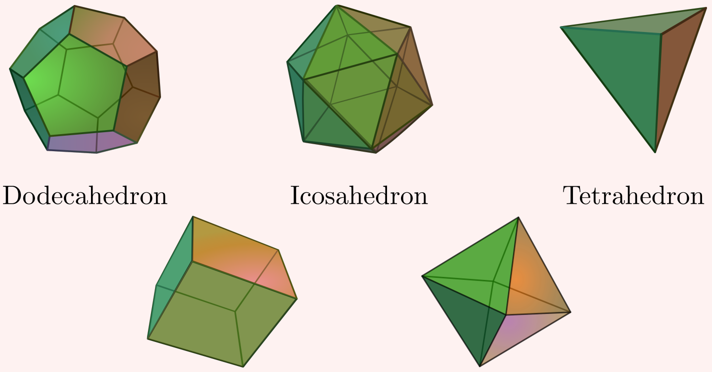
Consider a rectangle, then it has the following symmetries:

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.



Dodecahedron

Icosahedron

Tetrahedron

Hexahedron

Octahedron

The 5 regular Platonic solids.

We'll return to the notion of symmetric group and alternating group later, noting that the 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.

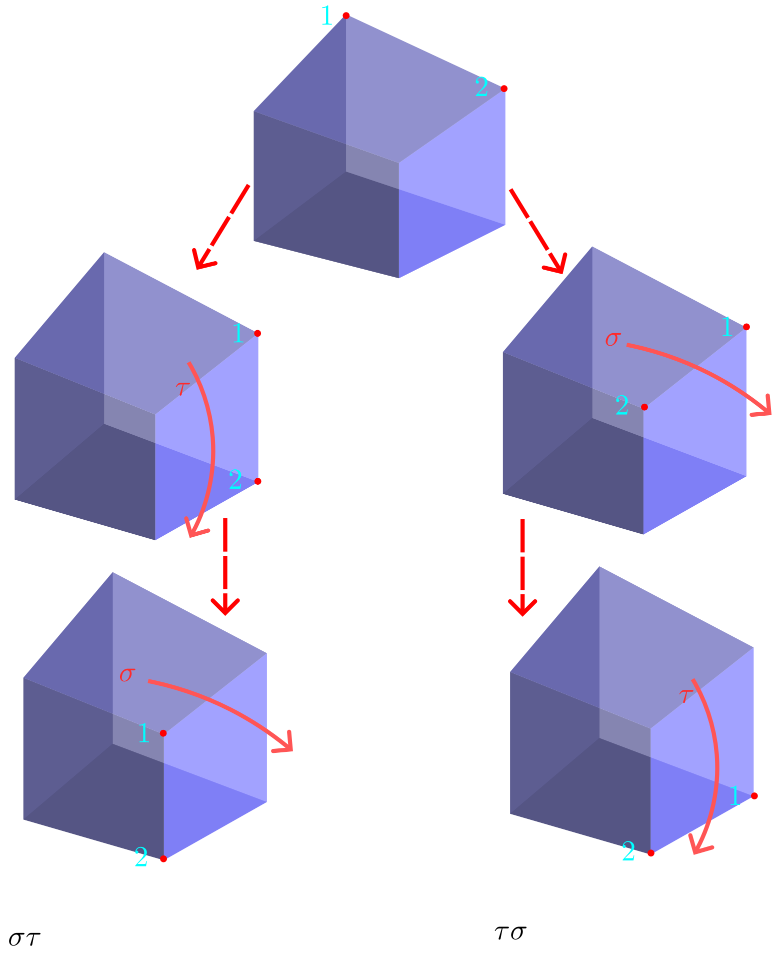


Figure 1: $\sigma\tau \neq \tau\sigma$

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

Definition 2.3

A **binary operation** on a set R is a function $* : R \times R \to R$, 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, $\ldots$, $q_n \in R$ assigned to it (although the same $q = r * s$ can coresspond 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 2.4 (Permutations)

Given a set X, a **permutation** of X is a bijective function $\sigma : X \to X$.

Remark. Then we use our concrete notion of a group to define what is called the *symmetric group*.

Definition 2.5 (Symmetric group)

The group of all permutations of X is denoted $\operatorname{Sym} X$, called the **symmetric group** on X. If $|X| = n$ for some $n \in \mathbb{Z}^+$, we write S_n for $\operatorname{Sym} X$. S_n is the **symmetric group on n elements**.

Remark. In particular $\operatorname{Sym} X$ has the following properties which shall be useful when we define an abstract group:

- *Closure.* The composition of two bijective functions from $X \to X$ is a bijective function from $X \to X$.
- *Associativity.* Composition of functions is associative.
- *Identity.* The identity function $\operatorname{id}(x) = x$ is bijective.
- *Inverses.* Every bijective function has a bijective inverse.

Definition 2.6 (Permutation group, or group of transformations)

A subset $T \subseteq \operatorname{Sym} X$ is called a **permutation group**, **group of transformations**, or **transformation group** iff T is a subgroup of $\operatorname{Sym} X$, i.e., T is itself a group.

It should be reasonably clear that $|\,\mathrm{S}_n\,| = n(n-1)\cdots 1 = n!$. We will also normally use $X = \{1, 2, 3, \dots, n\}$ when we study S_n. When dealing with permutation groups, it's helpful to have some notation to express permutations. For a general $\sigma \in S_n$, we write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

Example 2.3

If we had some $\sigma \in S_3$ such that $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$, we would write

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

A slightly better notation for when we have a permutation that 'cycles' some elements $a_1, \cdots a_k \in \{1, 2, \dots, n\}$ and leaves the other elements unchanged, we can write

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix}$$

which denotes the permutation mapping the elements as follows

$$\begin{tikzcd} a_1 \arrow[r] & a_2 \arrow[r] & a_3 \arrow[r] & \cdots \arrow[r] & a_k \arrow[llll, bend left] \end{tikzcd}$$

The cyclic nature of this notation also implies that the two permutations $(a_1\ a_2\ \cdots\ a_k) = (a_2\ a_3\ \cdots\ a_k\ a_1)$. To define this notation slightly more formally, we have

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix}(x) = \begin{cases} a_{i+1} & \text{if } x = a_i,\ (i < k) \\ a_1 & \text{if } x = a_k \\ x & \text{if } x \notin \{a_1, a_2, \dots, a_k\}. \end{cases}$$

We distinguish between permutations that can be written directly in this form in the following way.

Definition 2.7 (Cycles and Transpositions)

A permutation of the form $\sigma = (a_1\ a_2\ \cdots\ a_k)$ is a **k-cycle**. If $k = 2$ then we call it a **transposition**.

As cycles are permutations, we can compose them.

Example 2.4 (Composing Cycles)

If we consider the composition of two cycles $(1\ 2\ 3\ 4)(3\ 2\ 4)$, this should be a permutation in S_4. Indeed we have

$$\begin{aligned} 1 &\longmapsto 1 \longmapsto 2 \\ 2 &\longmapsto 4 \longmapsto 1 \\ 3 &\longmapsto 2 \longmapsto 3 \\ 4 &\longmapsto 3 \longmapsto 4 \end{aligned}$$

So we actually have that the composition of these cycles is also a cycle[a], namely $(1\,2\,3\,4)(3\,2\,4) = (1\,2)$.

[a] This is, in general, not the case

In the example above, the two cycles involved elements that were in both cycles. We have a specific term for when this is not the case.

Definition 2.8 (Disjoint Cycles)

We say that two cycles are **disjoint** if no number appears in both cycles.

Lemma 2.1

Disjoint cycles commute.

Proof. Let $\sigma, \tau \in S_n$ be two disjoint cycles. We want to show that $\sigma\tau = \tau\sigma$, that is, for any $x \in \{1, 2, \dots, n\}$, we have $\sigma(\tau(x)) = \tau(\sigma(x))$. We have two cases.

If x is in neither σ or τ, then $\sigma(x) = \tau(x) = x$, and thus $\sigma(\tau(x)) = \tau(\sigma(x)) = x$.

Otherwise x is in exactly one of σ or τ. WLOG let it be in σ. Then $\sigma(x)$ is also in σ (and hence not τ), so $\tau(x) = x$ and $\tau(\sigma(x)) = \sigma(x)$. Thus $\sigma(\tau(x)) = \sigma(x)$, so they commute. □

Slightly more surprising is the following theorem

Theorem 2.1 (Writing Permutations with Cycles)

Any $\sigma \in S_n$ can be written uniquely[a] as the composition of disjoint cycles.

[a] Up to the order of the cycles in the composition

Proof. First we show that any permutation can be written as the composition of cycles. Take $\sigma \in S_n$, and consider $1, \sigma(1), \sigma^2(1), \ldots$. Since $\{1, 2, \ldots, n\}$ is finite, there must exist $a > b$ such that $\sigma^a(1) = \sigma^b(1)$. So $\sigma^{a-b}(1) = 1$. Now let $k > 0$ be the smallest integer such that $\sigma^k(1) = 1$, which must exist by the previous argument. Then for $0 \leq l < m < k$, if $\sigma^m(1) = \sigma^l(1)$, then $\sigma^{m-l}(1) = 1$, which contradicts the minimality of k. So all of $1, \sigma(1), \sigma^2(1), \ldots, \sigma^k(1)$ are distinct. This gives us our first cycle $(1\ \sigma(1)\ \sigma^2(1)\ \sigma^{k-1}(1))$. We can repeat this process for the next number in $\{1, 2, \ldots, n\}$ that has not already appeared, until eventually every element has appeared. As σ is a bijection, no element can reappear.

We now show that this composition of cycles is unique up to the order of composition. Suppose we have two such decompositions

$$\begin{aligned}\sigma &= (a_1\ \cdots\ a_{k_1})(a_{k_{1+i}}\ \cdots\ a_{k_2})\cdots(a_{k_{m-1}}\ \cdots\ a_{k_m})\\ &= (b_1\ \cdots\ b_{k_1})(b_{k_{1+i}}\ \cdots\ b_{k_2})\cdots(b_{k_{m-1}}\ \cdots\ b_{k_m})\end{aligned}$$

and each $j \in \{1, 2, \ldots, n\}$ appears exactly once in both. Then we have $a_1 = b_t$ for some t, and the other numbers in the cycle are uniquely determined by $\sigma(a_1), \sigma^2(a_1), \ldots$. So we have

$$(a_1\ \cdots\ a_{k_1})(\cdots) = (b_t\ \cdots)(\cdots),$$

since disjoint cycles commute and we can 'cycle' the elements in cycles. If we continue this, we will find that all other cycles match too. □

Now let's consider an element $\sigma \in S_n$, and specifically we will look at the order of σ.

Definition 2.9

The set of cycle lengths of the disjoint cycle decomposition of a permutation σ is its **cycle type**.

Example 2.5

$(1\ 2\ 3)(5\ 6)$ has a cycle type of $3, 2$ (or $2, 3$).

Theorem 2.2

The order of $\sigma \in S_n$ is the least common multiple of the cycle lengths in its cycle type.

Proof. If $\sigma = \gamma_1\gamma_2\cdots\gamma_k$ is a decomposition of the permutation σ as a product of *disjoint* cycles, these cycles commute with each other. Hence $\sigma^r = \gamma_1^r\gamma_2^r\cdots\gamma_k^r$. and

$$\sigma^r = \gamma_1^r\gamma_2^r\cdots\gamma_k^r = e \iff \gamma_1^r = \gamma_2^r = \cdots = \gamma_k^r = e$$

whence r is a common multiple of $o(\gamma_1), o(\gamma_2), \dots, o(\gamma_k)$. The smallest of these r's is by definition the least common multiple of the orders of the cycles.

On the other hand, the order of a cycle is nothing but its length. □

This theorem gives us an easy way to find the order of the elements in S_n: write them in cycle notation.

Disjoint cycle notation is a useful way to express elements of S_n. Another useful notation is writing elements as the product of transpositions.

Theorem 2.3 (Writing Permutations with Transpositions)
Let $\sigma \in S_n$. Then σ is a product of transpositions.

Proof. It suffices to show that we can write any cycle as a product of transpositions. We observe that

$$\begin{pmatrix}a_1 & a_2 & \cdots & a_k\end{pmatrix} = \begin{pmatrix}a_1 & a_2\end{pmatrix}\begin{pmatrix}a_2 & a_3\end{pmatrix}\cdots\begin{pmatrix}a_{k-1} & a_k\end{pmatrix}.$$

□

Unlike the disjoint cycle decomposition, this isn't unique. For example, $(1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4) = (1\ 2)(2\ 3)(1\ 2)(3\ 4)(1\ 2)$. However, the pairity of the number of transpositions *is* invariant among decompositions.

Theorem 2.4 (Parity of Transpositions)
Writing $\sigma \in S_n$ as a product of transpositions in different ways, the number of transpositions used is always either even or odd, that is, the pairity is invariant with respect to σ.

Proof. Let's write $\chi(\sigma)$ for the number of cycles in σ in its disjoint cycle decomposition, including any 1-cycles. We will consider what happens to $\chi(\sigma)$ when we multiply σ by a transposition $\tau = (c\ d)$.

- If a cycle does not contain c or d, it will not be affected.
- If c and d are in the same cycle, say $(c\ a_2\ a_3\ \cdots\ a_{k-1}\ d\ a_{k+1}\ \cdots\ a_l)$, then composing with $(c\ \ d)$ gives $(c\ \ a_{k+1}\ \ \cdots\ \ a_l)(d\ \ a_2\ \ \cdots\ \ a_{k-1})$. So $\chi(\sigma\tau) = \chi(\sigma) + 1$.
- If c and d are in different cycles, we have

  $$(c\ a_2\ \cdots\ a_k)(d\ b_2\ \cdots\ b_l)(c\ d) = (c\ b_2\ \cdots\ b_e\ d\ a_2\ \cdots\ a_k).$$

  So $\chi(\sigma\tau) = \chi(\sigma) - 1$.

Thus for any σ and any transposition τ, $\chi(\sigma) \equiv \chi(\sigma\tau) + 1 \pmod 2$. We know that

$\chi(\sigma)$ is uniquely determined by σ, and if we write

$$\sigma = e\tau_1 \cdots \tau_k = e\tau_1' \cdots \tau_l',$$

we can use our result to get

$$\chi(\sigma) \equiv \chi(e) + k \equiv n + k \pmod 2$$
$$\chi(\sigma) \equiv \chi(e) + l \equiv n + l \pmod 2,$$

and thus $k \equiv l \pmod 2$. □

Because of this invariance, we can distinguish between odd and even permutations.

Definition 2.10 (Sign of a Permutation)

Writing $\sigma \in S_n$ as a product of transpositions $\sigma = \tau_1\tau_2 \cdots \tau_k$, the **sign** of σ is defined as $\operatorname{sgn}(\sigma) = (-1)^k$. If k is even, we say that σ is **even**, and if k is odd, we say that σ is **odd**.

Proposition 2.1

For $n \geq 2$, $\operatorname{sgn} : S_n \to \{\pm 1\}$ is an epimorphism.

Proof. We already know that sgn is well defined, and if $\chi(\sigma) = k$ and $\chi(\sigma') = l$ for $\sigma, \sigma' \in S_n$, then $\sigma\sigma'$ can be written with $k + l$ transpositions, so $\operatorname{sgn}(\sigma\sigma') = (-1)^{k+l} = (-1)^k(-1)^l = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma')$, so sgn is a homomorphism. It is also surjective since $\operatorname{sgn}(e) = 1$ and $\operatorname{sgn}(1\ 2) = -1$. □

There is an important group that comes from sgn being a homomorphism.

Definition 2.11 (Alternating Group)

The **alternating group** A_n is the kernel of the homomorphism $\operatorname{sgn} : \mathrm{S}_n \to \{\pm 1\}$, that is, it's the group of even permutations.

Theorem 2.5

$|A_n| = \frac{1}{2}|\,\mathrm{S}_n\,|$.

Proof. Let $B_n = S_n \setminus A_n \implies |A_n| + |B_n| = |S_n|$ as a permutation is either even or odd. Define $\varphi : A_n \to B_n$ s.t. $\varphi(a) = (1\ 2)a$. $(1\ 2)$ is odd and a is even so $(1\ 2)a$ is odd. Now,

$$\varphi(a) = \varphi(b) \implies (1\ 2)a = (1\ 2)b$$
$$\implies (1\ 2)(1\ 2)a = (1\ 2)(1\ 2)b \implies a = b.$$

Thus, φ is injective. Moreover,

$$y \in B_n \implies (1\ 2)y \in A_n$$

$$\implies \exists x = (1\ 2)y \in A_n : \varphi(x) = (1\ 2)x = (1\ 2)(1\ 2)y = y.$$

Thus, φ is surjective, so $\varphi : A_n \to B_n$ is a bijection. Thus

$$|A_n| = |B_n| = \frac{1}{2}|S_n|.$$

□

Theorem 2.6

For $n \geq 3$, A_n is generated by 3-cycles, or, equivalently, every even permutation is the product of 3-cycles.

Proof. Let $\alpha \in A_n$.

Then α is a product of $2m$ transpositions:

$$\alpha = \alpha_1 \cdots \alpha_{2m}.$$

As there are $2m$ transpositions, we can express α as the product of m pairwise products of transpositions

$$\alpha = \beta_1 \cdots \beta_m, \quad \beta_i = \alpha_{2i-1}\alpha_{2i}.$$

Each β_i is the product of 2 transpositions, so either

$$\begin{aligned} \beta_i &= (a\ b)(c\ d) \\ &= (a\ c\ b)(c\ d\ a). \end{aligned}$$

or

$$\begin{aligned} \beta_i &= (a\ b)(b\ c) \\ &= (a\ c\ b). \end{aligned}$$

So, either β_i is a 3-cycle or it is the product of 3-cycles.

So α is a product of 3-cycles. □

§2.3 Abstract groups

Definition 2.12 (Abstract group)

A **group** is a set G with a binary operation $G \times G \to G$ (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

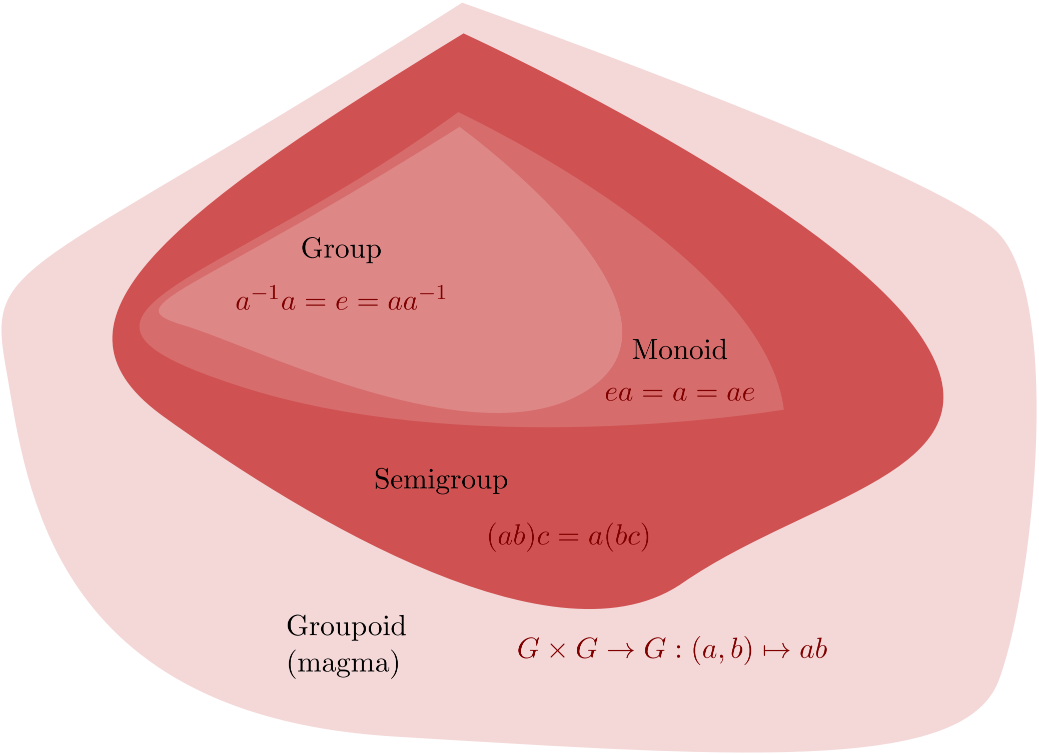


Figure 2: Some abstract algebraic structures

Definition 2.13 (Subgroup)

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

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 2.14

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

$$ab = ba$$

for every a, $b \in G$.

Definition 2.15 (Order and Cayley table)

The **order** of a group is the number of elements in it, and if the order of a group is finite then the group is called a finite group.

For a finite group $G = \{a_1 = e, a_2, \dots, a_n\}$, we can draw a multiplication table, called **Cayley table**, as follows

$$\begin{array}{c|cccccc} \cdot & e & a_2 & \dots & a_j & \dots & a_n \\ \hline e & & & & & & \\ \vdots & & & & \vdots & & \\ a_i & & & \dots & a_i a_j & \dots & \\ \vdots & & & & \vdots & & \\ a_n & & & & & & \end{array}$$

where $a_i a_j$ is tabulated in the intersection of the row headed by a_i and column headed by a_j.

There are many examples of groups.

Example 2.6

(Exercise: Show that the following examples satisfy or do not satisfy the group axioms, whichever is applicable, explicitly.)

1. The **trivial group** is the set $\{e\}$ containing just the identity.
2. The set $\operatorname{Sym} X$ 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:

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

The set of *even* permutations, called the **alternating group A_n**, is the kernel of the homomorphism

$$\operatorname{sgn} : \mathrm{S}_n \to \{\pm 1\},$$

and

$$|A_n| = \frac{1}{2}|S_n|.$$

3. 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.

4. Consider the same set as above, but with matrix product $\cdot : M_n(\mathbb{F}) \times M_n(\mathbb{F}) \to M_n(\mathbb{F})$, $(A, B) \mapsto P$ defined by

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

So,

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

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.

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

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

with the operation of matrix multiplication. If $A, B \in \mathrm{GL}_n(\mathbb{F})$ 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, $\mathrm{GL}_n(\mathbb{F})$ forms a nonabelian group, called the **general linear group**.

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

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

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

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

7. The group of orthogonal matrices of order n over a field $\mathbb{F}$ is the **orthogonal group**

$$\mathrm{O}_n(\mathbb{F}) = \{A \in \mathrm{GL}_n(\mathbb{F}) : A^T A = I\}.$$

Similarly, the **special orthogonal group** is the group

$$\mathrm{SO}_n(\mathbb{F}) = \{A \in \mathrm{SL}_n(\mathbb{F})\}.$$

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 $\varnothing$ as the zero element and with every element being its own inverse. Also, $(2^X, \cap)$ is a semigroup.

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

10. The **circle group** $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. One of its subgroups is the group of n^{th} roots of unity $U_n = \{z \in \mathbb{C} : z^n = 1\}$. Both are cyclic groups (in fact the term originated from the fact that U_n is a subgroup of S^1).

11. 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 $n \in \mathbb{Z}$. It is an infinite cyclic group. 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.

12. The integers modulo m, $\mathbb{Z}_m = \{0, \dots, m-1\}$, is an abelian group under addition but not under multiplication; however,

$$\mathbb{Z}/m\mathbb{Z} = \{n \in \mathbb{Z}_m : \gcd(n, m) = 1\}.$$

so that each element is co-prime to m is indeed a group under multiplication, called the **multiplicative group of integers modulo m.** These are also examples of cyclic groups.

13. The **quaternion group $\mathbb{Q}_8$** consisting of the matrices $\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ defined as,

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

where

$$\mathbf{i}^{\mathbf{2}} = \mathbf{j}^{\mathbf{2}} = \mathbf{k}^{\mathbf{2}} = -\mathbf{1}, \;\; \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \mathbf{ki} = -\mathbf{ik} = \mathbf{j},$$

is a noncommutative group of order 8.

14. The **Klein 4-group $\mathcal{K}_4$** is the abelian group of symmetries of a rectangle which is not a square, or the group

$$\mathcal{K}_4 = \{e, a, b, ab\}$$

given by the multiplication table

$\cdot$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

15. A symmetry of a regular n-gon is a transformation of the n-gon, so that when the transformed n-gon is placed on the original n-gon, it exactly covers it. The **dihedral group $\mathcal{D}_{2n}$** is the group of symmetries of a regular n-gon under the operation of composition of symmetries. As the subscript suggests, a regular n-gon has $2n$ symmetries so $|\mathcal{D}_{2n}| = 2n$.

Lemma 2.2

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. (i) Either left or right multiplying by x^{-1} yields $a = b$ in both cases.

(ii) Let $ea = ae = a,\ e'a = ae' = a$. Then $a = a \implies ae = ae' \implies e = e'$.

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

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

(iv) $a^{-1}(a^{-1})^{-1} = e \overset{\text{left multiply by } a}{\implies} (a^{-1})^{-1} = a$. □

Definition 2.16 (Centraliser and center)

Let G be a group. The **centraliser** $C(a)$ of $a \in G$ is the set of elements in G that commute with a,

$$C(a) = \{g \in G : ga = ag\} = \{g \in G : gag^{-1} = a\}.$$

The **center** $Z(G)$ (from German *Zentrum*) of G is the set of elements in G that commute with every element in G,

$$Z(G) = \{g \in G : gh = hg\ \forall h \in G\} = \{g \in G : ghg^{-1} = h\ \forall h \in G\}.$$

Theorem 2.7

$C(a),\ Z(G)$ are subgroups of G.

Proof. $ea = ae$ for all $a \in G$ so $e \in Z(G)$. If $x,\ y^{-1} \in Z(G)$ then

$$xhx^{-1} = h,\ y^{-1}hy = h$$

for every $h \in G$. Thus,

$$xy^{-1}h(xy^{-1})^{-1} = x(y^{-1}hy)x^{-1} = xhx^{-1} = h\ \forall h \in G.$$

So $x,\ y^{-1} \in Z(G) \implies xy^{-1} \in Z(G)$. Thus, $Z(G)$ is a subgroup of G.

$ea = ae$ so $e \in C(a)$. Again, if $x,\ y^{-1} \in C(a)$ then

$$xax^{-1} = a,\ y^{-1}ay = a.$$

Thus,

$$xy^{-1}a(xy^{-1})^{-1} = x(y^{-1}ay)x^{-1} = xax^{-1} = a.$$

So $xy^{-1} \in C(a)$. Thus $C(a)$ is a subgroup of G.

Note that $g \in Z(g) \implies g \in C(A) = \{g \in G : ga = ag\ \forall a \in A\}$ so center is a subgroup of centraliser. □

§2.4 Cayley's theorem

Notation. If a homomorphism $\eta : A \to B$ is an isomorphism, then we write $A \cong B$.

Theorem 2.8 (Cayley's Theorem)

Every group G is isomorphic to a transformation group, i.e. a subgroup of the symmetric group $\operatorname{Sym} G$.

Proof. Recall that the symmetric group $\operatorname{Sym} G$ is the group of all bijections $\eta : G \to G$. Define $T_a : G \to G$ for some $a \in G$ as the map $T_a(x) = ax$, for all $x \in G$. Then there exists the inverse map $T_a^{-1}(x) = T_{a^{-1}}(x) = a^{-1}x$ s.t. $T_a^{-1}(T_a(x)) = x$. Thus, $T_a : G \to G$ is a bijection so that $T_a \in \operatorname{Sym} G \; \forall a \in G$. Let $K = \{T_a : a \in G\}$, then K is a subgroup of $\operatorname{Sym} G$.

Now consider $f : G \to K$ s.t. $f(a) = T_a$ for all $a \in G$. Then

$$f(ab) = T_{ab}(x) = (ab)x = a(bx) = T_a(T_b(x)) = (T_a \circ T_b)(x) = f(a)f(b).$$

So f is a homomorphism. Now,

$$f(a) = f(b) \implies T_a(x) = T_b(x) \implies ax = bx \implies a = b.$$

So f is injective. Moreover, for every $T_a \in K$ there exists $a \in G : f(a) = T_a$. So f is surjective, and thus f is an isomorphism so that

$$G \cong K, \text{ a subgroup of } \operatorname{Sym} G.$$

□

§2.5 Cyclic groups

Remark. We have already seen some examples of cyclic groups, which we shall now define:

Definition 2.17 (Cyclic group)

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 2.9 (Classification of all cyclic groups)

Let $G = \langle a \rangle$. If $|G| = n < \infty$ then $G \cong \mathbb{Z}_n$. Otherwise, if $|G| = \infty$, then $G \cong (\mathbb{Z}, +)$.

Proof. If G is finite of order n consider the map $\eta : G \to \mathbb{Z}_n$ defined by

$$\eta(a^k) = [k]_n, \; k \in \mathbb{Z}.$$

Then $\eta(a^{j+k}) = [j+k]_n = [j]_n + [k]_n = \eta(a^j) + \eta(a^k)$. So it is a homomorphism.

Now, $\eta(a^k) = \eta(a^j) \implies [j]_n = [k]_n$ so it is injective. Also for any $[k]_n \in \mathbb{Z}_n$ there exists $a^k \in G : \eta(a^k) = [k]_n$ so it is surjective. Thus η is an isomorphism, therefore $G \cong \mathbb{Z}_n$.

If G is infinite then consider the map $\mu : G \to (\mathbb{Z}, +)$ defined by

$$\mu(a^k) = k,\ k \in \mathbb{Z}.$$

Then $\mu(a^{j+k}) = j + k = \mu(a^j) + \mu(a^k)$. So it is a homomorphism.

Now, $\eta(a^k) = \eta(a^j) \implies j = k$ so it is injective. Also for any $k \in \mathbb{Z}$ there exists $a^k \in G : \eta(a^k) = k$ so it is surjective. Thus η is an isomorphism, therefore $G \cong (\mathbb{Z}, +)$. □

Theorem 2.10

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

Proof. Sps G is a cyclic group with generator a, i.e., $G = \langle a \rangle$. Let H be a subgroup of G. If $H = \langle e \rangle$ then it is the trivial group and trivially cyclic. So sps $H \neq \langle e \rangle$. Let $n > 0$ be the least positive integer s.t. $a^n \in H$. As H is a subgroup, $\langle a^n \rangle \subseteq H$. If b is an arbitrary element of H, then as $b \in G$, we have $b = a^m$ for some $m \in \mathbb{Z}^+$. By the division algorithm we can write

$$m = nq + r,\ q, r \in \mathbb{Z} : 0 \leq r < n.$$

Then

$$b = a^{nq+r} = (a^n)^q \cdot a^r$$

$$\implies a^r = a^m \cdot (a^n)^{-q} \implies a^r \in H.$$

If $r > 0$ then it contradicts the minimality of n. Thus $r = 0$, so that

$$b = a^m = (a^n)^q.$$

As b was arbitrarily chosen, this shows that $H \subseteq \langle a^n \rangle$. But $\langle a^n \rangle \subseteq H$, so $H = \langle a^n \rangle$. □

§2.6 Cosets

Definition 2.18 (Left and right cosets)

For a group G and a subgroup H of G, we define a **left coset** of H in G to be the set $aH = \{ah : h \in H\}$ for some $a \in G$. Similarly, a **right coset** of H generated by $a \in G$ is the set $Ha = \{ha : h \in H\}$.

The number of distinct left cosets of H in G is called the **index [G:H]** of H in G.

Theorem 2.11 (Coset Properties)

Let H be a subgroup of G and $a, b \in G$.

(i) $aH = H \iff a \in H$.

(ii) $aH = bH \iff a^{-1}b \in H$.

Proof. (i) If $aH = H$, then $a = ae \in aH = H$ (because $e \in H$). For the converse, let $a \in H$. As H is closed, $aH \subseteq H$. Now, let $h \in H$. Then $a^{-1}h \in H$ as H is a subgroup of G. Then

$$h = eh = (aa^{-1})h = a(a^{-1}h) \in aH.$$

Thus $H \subseteq aH$, so $aH = H$.

(ii) $aH = bH$ can be written as $a^{-1}bH = a^{-1}aH = eH = H$. Then applying the above result we get what was to be shown.

□

Theorem 2.12 (Lagrange)

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

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

Proof. G finite $\implies$ $[G : H]$ finite. Set $[G : H] = r$. So there are r distinct left cosets $a_1H, a_2H, \ldots, a_rH$ of H in G. Distinct left cosets are pairwise disjoint, and $h \mapsto a_ih$ is a bijection between H and a_iH. Thus,

$$\begin{aligned} |G| = \left|\bigcup_{i=1}^{r} a_iH\right| &= \sum_{i=1}^{r} |a_iH| \\ &= \sum_{i=1}^{r} |H| = r|H|. \end{aligned}$$

Thus, $|G| = |H|[G : H]$. □

Corollary 2.1

If G is a finite group of prime order p, then G is cyclic.

Proof. As $p > 1$ there exists $a \neq e \in G$. Let H be the cyclic subgroup of G generated by a. Then $o(H) \mid o(G) = p \implies o(H) = 1, p$. But $a \neq e$ so $o(H) = p$. Now $H \subseteq G$, $|H| = p = |G| \implies G = H$. So G is cyclic. □

Corollary 2.2

If G is a finite group of order n, then $o(a) \mid n$ and $a^n = e$ for every $a \in G$.

Proof. Let $a \in G$ and let $m = o(a)$. Then $a^m = e$. Let H be the cyclic subgroup of G generated by a. Then $o(H) = o(a) = m$. As $o(H) \mid o(G)$ we have $o(a) \mid n$. So $m = o(a) = nk$ for some $k \in \mathbb{Z}$. Now $a^n = (a^m)^k = e^k = e$. □

Remark. Lagrange's Theorem readily gives us the following two results from number theory.

Theorem 2.13 (Fermat's Little Theorem)

Let p be prime and $a \in \mathbb{Z} : \ \gcd(a, p) = 1$. Then,

$$a^{p-1} \equiv 1 \mod p.$$

Proof. Consider the multiplicative group of integers modulo p, $\mathbb{Z}/p\mathbb{Z}$, and as p is prime we have $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p \setminus \{[0]\}$ of order $p-1$. Let $a \in \mathbb{Z} : \ \gcd(a, p) = 1$. Then $[a] \in \mathbb{Z}/p\mathbb{Z}$. By Corollary 2.2, we have $[a]^{p-1} = [1] \implies a^{p-1} \equiv 1 \pmod{p}$. □

Definition 2.19

We define **Euler's totient function** $\phi(n)$ for an integer $n \in \mathbb{Z}^+$ with prime factorisation $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ as

$$\phi(n) = p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1) \cdots p_r^{k_r-1}(p_r - 1).$$

This counts the number of integers $\leq n$ coprime to n.

Theorem 2.14 (Euler)

Let $a, n \in \mathbb{Z} : \ n > 0, \ \gcd(a, n) = 1$. Then

$$a^{\phi(n)} \equiv 1 \mod n.$$

Proof. For $\mathbb{Z}/n\mathbb{Z}$ we have $o(\mathbb{Z}/n\mathbb{Z}) = \phi(n)$ by definition. Let $a \in \mathbb{Z} : \ \gcd(a, n) = 1$. Then $[a] \in \mathbb{Z}/n\mathbb{Z}$.
By Corollary 2.2, we have $[a]^{\phi(n)} = [1] \implies a^{\phi(n)} \equiv 1 \pmod{n}$. □

Theorem 2.15

Let H and K be finite subgroups of G. Then,

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. $A = H \cap K$ is a subgroup of G and, in particular, H. By Lagrange's Theorem, $o(A) \mid o(H)$. Let $n = \frac{|H|}{|A|} \implies [H : A] = n$ so A has n distinct left cosets $x_1A, x_2A, \ldots, x_nA$ in H. As $A \subseteq K$ and $H = \bigcup_{i=1}^{n} x_iA$, we have

$$HK = \left(\bigcup_{i=1}^{n} x_iA \right) K = \bigcup_{i=1}^{n} x_iK.$$

We now show that $x_iK \cap x_jK = \varnothing, \ i \neq j$ (pairwise disjoint).
$x_iK \cap x_jK \neq \varnothing, \ i \neq j \implies x_iK = x_jK \implies x_i^{-1}x_j \in K$. As $x_i^{-1}x_j \in H$ we have $x_i^{-1}x_j \in A$ so $x_iA = x_jA$. This contradicts our assumption that the cosets $x_1A, x_2A, \ldots, x_nA$ are distinct. So $x_1K, x_2K, \ldots, x_nK$ are distinct left cosets of K.

Thus, $|K| = |x_iK|$, and we have

$$\begin{aligned} |HK| = \left| \bigcup_{i=1}^{n} x_iK \right| &= \sum_{i=1}^{n} |x_iK| \\ = \sum_{i=1}^{n} |K| = n|K| &= \frac{|H|}{|A|}|K| \\ &= \frac{|H||K|}{|H \cap K|}. \end{aligned}$$

□

§2.7 Direct product

Remark. The direct product is a generalisation of the Cartesian product to groups.

Definition 2.20 (Direct product)

The **(external) direct product $G \times H$** of two group G and H is the set $G \times H$ with the operation $\cdot$ defined componentwise: $(a, b) \cdot (c, d) = (a \cdot b, c \cdot d)$. This is then associative, has the identity element (e_G, e_H), and (g^{-1}, h^{-1}) is the inverse for each $(g, h) \in G \times H$. Thus, the external direct product $G \times H$ is a group.

Let G be a group and H and K subgroups of G. Then G is the **internal direct product of H and K** iff

(i) $G = HK$.

(ii) $H \cap K = \{e\}$.

(iii) $hk = kh$ for all $h \in H$ and $k \in K$.

Theorem 2.16

Let G be a group and H and K subgroups of G. Then G is the *internal direct product of H and K* iff

(i) $G = HK$.

(ii) $H, K \trianglelefteq G$.

(iii) $H \cap K = \{e\}$.

Proof. $\underline{\Longrightarrow}$: Let G be the internal direct product of H and K and let $g \in G$, $h \in H$. As $G = HK$ there exist $h_1 \in H$, $k_1 \in K : g = h_1k_1$. Now, $ghg^{-1} = h_1k_1hk_1^{-1}h_1^{-1} = h_1hk_1k_1^{-1}h_1^{-1}$ (using $hk = kh$). Thus $ghg^{-1} = h_1hh_1^{-1}$ so $H \trianglelefteq G$. Similarly, we also have $K \trianglelefteq G$.

$\underline{\Longrightarrow}$: Let (i), (ii), (iii) hold. Then we need to show $ab = ba$ for all $a \in H$ and $b \in K$. Consider $aba^{-1}b^{-1}$. Then

$$aba^{-1}b^{-1} \in a(bHb^{-1}) \subseteq aH = H, \; aba^{-1}b^{-1} \in (aKa^{-1})b^{-1} \subseteq Kb^{-1} = K.$$

Thus $aba^{-1}b^{-1} \in H \cap K = \{e\} \implies ab = ba$. □

Theorem 2.17

The direct product $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

Proof. Assume towards a contradiction that $\mathbb{Z} \times \mathbb{Z}$ is cyclic with generator (n, m). We have $(0,1), (1,0) \in \mathbb{Z} \times \mathbb{Z}$. Thus there exist $r, s \in \mathbb{Z}$:

$$(1,0) = r(n,m), \ (0,1) = s(n,m).$$

But $rn = 1$ and $sn = 0$ imply $s = 0$ so that $1 = sm = 0$. Absurdity. Thus, $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. □

Theorem 2.18

$(\mathbb{R}^*, \cdot) = \mathbb{R}^+ \times T, \ T = \{\pm 1\}$.

Proof. Let $a \in \mathbb{R}^*$. If $a > 0$ then $a = a \cdot 1 \in \mathbb{R}^+ T$, and if $a < 0$ then $a = (-a) \cdot (-1) \in \mathbb{R}^+ T$. So $\mathbb{R}^* = \mathbb{R}^+ T$. Moreover, $\mathbb{R}^+ \cap T = \{1\}$ and $ab = ba$ for all $a \in \mathbb{R}^+, \ b \in T$. Thus, $(\mathbb{R}^*, \cdot) = \mathbb{R}^+ \times T$ is an internal direct product. □

Theorem 2.19

The direct product $H \times K$ of two finite cycle groups H and K with $|H| = m, |K| = n$ is cyclic iff $\gcd(m, n) = 1$.

Proof. Assume that $H \times K$ is cyclic and let $\gcd(m, n) = d > 1$. For any $a \in H, b \in K$ we have $a^m = e$ and $b^n = e$ as $|H| = m, \ |K| = n$. Also $\gcd(m, n) = d > 1 \implies \frac{mn}{d} \in \mathbb{Z}^+$. Now,

$$\begin{aligned}(a,b) \in H \times K \implies (a,b)^{\frac{mn}{d}} &= (a^{\frac{mn}{d}}, b^{\frac{mn}{d}}) \\ &= ((a^m)^{\frac{n}{d}}, (b^n)^{\frac{m}{d}}) \\ &= (e,e).\end{aligned}$$

Thus, the order of every $(a,b) \in H \times K$ is at most $\dfrac{mn}{d} < mn$. Then $H \times K$, a group of order mn, contains no element of order mn, contradicting our assumption that $H \times K$ is cyclic. Thus $\gcd(m, n) = 1$.

Assume that $\gcd(m, n) = 1$. As H and K are cyclic of order m and n, for any $a \in H, \ b \in K$ we have $a^m = e$ and $b^n = e$. Thus,

$$\begin{aligned}(a,b) \in H \times K \implies (a,b)^{mn} &= (a^{mn}, b^{mn}) \\ &= ((a^m)^n, (b^n)^m) \\ &= (e,e).\end{aligned}$$

Thus, the order of every $(a,b) \in H \times K$ is at most mn. Let $d \in \mathbb{Z}^+ : d \leq mn$ s.t. $(a,b)^d = (e,e)$. Then $a^d = e, \ b^d = e$. As $o(a) = m, \ o(b) = n$ we have $m \mid d$ and

> $n \mid d$, but $\gcd(m,n)=1$ thus $d=mn$ and thus the order of every $(a,b) \in H \times K$ is $mn \implies H \times K$ is cyclic of order mn. □

§2.8 Congruences and quotient groups

Remark. We know from number theory that two integers a and b are defined to be congruent modulo the integer m, denoted as $a \equiv b \pmod{m}$, iff $a-b$ is a multiple of m:

$$a - b = km, \; k \in \mathbb{Z}.$$

The relation between a and b thus defined for fixed m is an equivalence relation; for, we have

1. $a \equiv a \pmod{m}$. (*reflexive*)
2. $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$. (*symmetric*)
3. $a \equiv b \pmod{m}$, $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$. (*transitive*)

These congruences $(\mathbb{Z}_m, +)$ and $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ are examples of a general notion which we shall now define.

Definition 2.21 (Congruence relation)

Let G be a group. A **congruence (relation)** $\equiv$ in G is an equivalence relation such that for any $a, a', b, b' : \; a \equiv a', \; b \equiv b'$, we have $ab \equiv a'b'$. In other words, congruences are equivalence relations which can be multiplied.

Remark. Let $\equiv$ be a congruence in the group G and consider the quotient set $\overline{G} = G/\equiv$ of G relative to $\equiv$. Note that the quotient set is the subset $\overline{G} \subseteq \mathcal{P}(G)$ consisting of the equivalence classes $\overline{a} = \{b \in G : b \equiv a\}$. In general, if $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$, then $\overline{ab} = \overline{a'b'}$. Hence the map $(\overline{a}, \overline{b}) \to \overline{ab}$ is a well-defined binary operation on $\overline{G}$. Then $(\overline{G}, \cdot)$ is a group (exercise: verify!) called the *quotient group of G relative to the congruence $\equiv$*. For example, the quotient group $\mathbb{Z}/m\mathbb{Z}$ consists of m elements:

$$\begin{aligned}
&[0]_m = \overline{0} = \{0, \pm m, \pm 2m, \pm 3m, \dots\} \\
&[1]_m = \overline{1} = \{1, 1 \pm m, 1 \pm 2m, 1 \pm 3m, \dots\} \\
&\vdots \\
&[m-1]_m = \overline{m-1} = \{m-1, m-1 \pm m, m-1 \pm 2m, m-1 \pm 3m, \dots\}.
\end{aligned}$$

Definition 2.22 (Normal subgroup)

A subgroup K of a group G is said to be **normal** iff $gK = Kg$ for all $g \in G$. We then write $K \trianglelefteq G$.

Remark. The fundamental connection between normal subgroups of G and congruences on G is given by the following theorem:

Theorem 2.20

Let G be a group and $\equiv$ a congruence on G. Then the congruence class $K = \overline{1}$ of the identity is a normal subgroup of G and for any $g \in G$,

$$\overline{g} = gK = Kg,$$

the right or left coset of g relative to K. Conversely, let $K \trianglelefteq G$, then $\equiv$ defined by

$$a \equiv b \pmod{K} \text{ iff } a^{-1}b \in K$$

is a congruence relation in G whose associated congruence classes are the left (or right) cosets gK.

Proof. Suppose that we have a congruence $\equiv$ on G and let $K = \overline{1}$. Then,
$k_1, k_2 \in K \implies \overline{k_1 k_2^{-1}} = \overline{k_1 k_2}^{-1} = \overline{1 1}^{-1} = \overline{1} \implies k_1 k_2 \in K$.
So K is a subgroup of G.

Now, let $g \in G$ and consider the congruence class $\overline{g}$. Then,

$$a \in \overline{g} \implies g^{-1}a,\ ag^{-1} = \overline{1} \in K,$$

$$\implies a \in gK,\ a \in Kg.$$

Conversely, let $a \in Kg$. Then, $\overline{a} = \overline{kg} = \overline{1}\overline{g} = \overline{g}$ so $a \equiv g$. Same holds for $a \in gK$. Thus,

$$\overline{g} = gK = Kg.$$

Conversely, let $K \trianglelefteq G$ and define $a \equiv b \pmod{K}$ to mean $a^{-1}b \in K$, i.e., $b \in aK$. This relation $\equiv$ is an equivalence relation, and if $a \equiv g \pmod{K}$ and $b \equiv h \pmod{K}$ then for some k_i's $\in K$ we have $a = gk_1,\ b = hk_2$ and since $hK = Kh$ we have $hk_3 = k_1 h$. Thus, $ab = gk_1hk_2 = ghk_3k_2$ so $ab \equiv gh \pmod{K}$. Thus $\equiv$ is a congruence relation in G with $\overline{1} = \{k : 1^{-1}k \in K\} = K$ and $\overline{g} = \{a : g^{-1}a \in K\} = gK$ for any $g \in G$. □

Remark. We shall now write G/K for $\overline{G} = G/\equiv \pmod{K}$ which we call the *factor group* (or *quotient group*) of G relative to the normal subgroup K.

Definition 2.23 (Quotient group)
Let G be a group and $K \trianglelefteq G$. The **quotient group** G/K is defined as the group of left cosets of the normal subgroup K in G,

$$G/K = \{aK : a \in G\},$$

with $aK \cdot bK = abK$.

Definition 2.24 (Centraliser and normaliser)
The **centraliser** $C(A)$ of $A \subseteq G$ is the set of elements in G that commute with every element $a \in A$,

$$C(A) = \{g \in G : ga = ag\ \forall a \in A\} = \{g \in G : gag^{-1} = a\ \forall a \in A\}.$$

The **normaliser** $N(A)$ of $A \subseteq G$ is the set of elements in G such that for every

$a \in A$ there is some $a' \in A$ s.t. $gag^{-1} = a'$,

$$N(a) = \{g \in G : gAg^{-1} = A\} = \{g \in G : gA = Ag\}.$$

Definition 2.25 (Conjugacy class)

The **conjugacy class** $\mathrm{ccl}(a)$ of an element $a \in G$ in a group G is the set

$$\mathrm{ccl}(a) = \{gag^{-1} : g \in G\}.$$

Theorem 2.21

gHg^{-1} is a subgroup of G for all $g \in G$.

Proof. $e = geg^{-1} \in gHg^{-1}$. Let $a, b \in H$ with gag^{-1}, $gbg^{-1} \in gHg^{-1}$. Then $(gbg^{-1})^{-1} = gb^{-1}g^{-1}$. Then $gag^{-1}gb^{-1}g^{-1} = gab^{-1}g^{-1} \in gHg^{-1}$. Thus, gHg^{-1} is a subgroup of G. □

Theorem 2.22

The following are equivalent:

(i) $K \trianglelefteq G$.

(ii) $gKg^{-1} \subseteq K \; \forall g \in G$.

(iii) $gKg^{-1} = K \; \forall g \in G$.

Proof. **(i) $\implies$ (ii):**

Let $K \trianglelefteq G$. Let $g \in G$. Then $gK = Kg$. Thus, for any $k \in K$, $gk \in gK = Kg \implies gk = k'g$ for some $k' \in K$. Thus $gkg^{-1} = k' \in K$. Thus, $gKg^{-1} \subseteq K$.

(ii) $\implies$ (iii):

Let $k \in K$. Then $g^{-1}k(g^{-1})^{-1} \in g^{-1}K(g^{-1})^{-1} \subseteq K$. Also $k = g(g^{-1}kg)g^{-1} \in gKg^{-1}$. So

$$K \subseteq gKg^{-1} \subseteq K \implies gKg^{-1} = K.$$

(iii) $\implies$ (i):

Since $gKg^{-1} = K$, $\forall g \in G$ we find that $gK = Kg$, $\forall g \in G$. Thus $K \trianglelefteq G$. □

We end this section with Cauchy's Theorem on Finite Abelian Groups:

Theorem 2.23 (Cauchy)

Let G be a finite abelian group and p be a prime dividing $|G|$, then G contains an element of order p.

Proof. We will prove this lemma by induction. If $n = 1$, then there is nothing to show. Now suppose that the lemma is true for all groups of order k, where $k < n$. Furthermore, let p be a prime that divides n.

If G has no proper nontrivial subgroups, then $G = \langle a \rangle$, where a is any element other than the identity. By Exercise 4.5.39, the order of G must be prime. Since p divides n, we know that $p = n$, and G contains $p - 1$ elements of order p.

Now suppose that G contains a nontrivial proper subgroup H. Then $1 < |H| < n$. If $p \mid |H|$, then H contains an element of order p by induction and the lemma is true. Suppose that p does not divide the order of H. Since G is abelian, it must be the case that H is a normal subgroup of G, and $|G| = |H| \cdot |G/H|$. Consequently, p must divide $|G/H|$. Since $|G/H| < |G| = n$, we know that G/H contains an element aH of order p by the induction hypothesis. Thus,

$$H = (aH)^p = a^p H,$$

and $a^p \in H$ but $a \notin H$. If $|H| = r$, then p and r are relatively prime, and there exist integers s and t such that $sp + tr = 1$. Furthermore, the order of a^p must divide r, and $(a^p)^r = (a^r)^p = 1$.

We claim that a^r has order p. We must show that $a^r \neq 1$. Suppose $a^r = 1$. Then

$$\begin{aligned} a &= a^{sp+tr} \\ &= a^{sp} a^{tr} \\ &= (a^p)^s (a^r)^t \\ &= (a^p)^s 1 \\ &= (a^p)^s. \end{aligned}$$

Since $a^p \in H$, it must be the case that $a = (a^p)^s \in H$, which is a contradiction. Therefore, $a^r \neq 1$ is an element of order p in G. □

§2.9 Homomorphisms revisited and the first isomorphism theorem

Proposition 2.2 (Homomorphism preserves identity)

Let $\eta : A \to B$ be a homomorphism between two groups A and B with identities e and e' respectively. Then $\eta(e) = e'$.

Proof. We have, by definition of homomorphism,

$$\eta(e) = \eta(e^2) = \eta(e)^2,$$

and multiplying by $\eta(e)^{-1}$ we obtain $\eta(e) = e'$. □

Lemma 2.3

A homomorphism between two groups $\eta : A \to B$ is a monomorphism iff $\ker \eta = \{e\}$.

Proof. As η is homomorphism, $\eta(e) = e$.

$\implies$:

As η is a monomorphism, $\eta(x) = \eta(e) \implies x = e$. So $\ker \eta = \{e\}$.

$\impliedby$:

As $\ker \eta = \{e\}$, we have $\eta(x) = e \implies x = e$. Now,

$$\eta(a) = \eta(b)$$
$$\implies \eta(a^{-1})\eta(a) = \eta(a^{-1})\eta(b) \implies \eta(e) = \eta(a^{-1}b) \implies e = a^{-1}b$$
$$\implies a = b.$$

So, η is a monomorphism. □

Lemma 2.4

Let $\eta : A \to B$ be a homomorphism between two groups. Then, $\operatorname{im} \eta$ is a subgroup of B and $\ker \eta$ is a normal subgroup of A, i.e. $\ker \eta \trianglelefteq A$.

Proof. $\eta(e) = e$ so $e \in \operatorname{im} \eta$. Let $\eta(a),\ \eta(b) \in \operatorname{im} \eta$.

$$\begin{aligned} \implies \eta(a)\eta(b)^{-1} &= \eta(a)\eta(b^{-1}) \\ &= \eta(ab^{-1}) \in \operatorname{im} \eta. \end{aligned}$$

Thus $\operatorname{im} \eta$ is a subgroup of B.

Recall that $\ker \eta = \{a \in A : \eta(a) = e\}$. Clearly $\eta(e) = e$ so $e \in \ker \eta$. Now, let $a, b \in \ker \eta \implies \eta(a) = \eta(b) = e$. Clearly, $\eta(b^{-1}) = \eta(b^{-1})\eta(b) = \eta(b^{-1}b) = \eta(e) = e$, so $\eta(ab^{-1}) = \eta(a)\eta(b^{-1}) = e \implies ab^{-1} \in \ker \eta$. Thus $\ker \eta$ is a subgroup of A. Now, fix $k \in \ker \eta$, so $\eta(k) = e$. Let $a \in A$. Then

$$\eta(aka^{-1}) = \eta(a)\eta(k)\eta(a^{-1}) = \eta(a)\eta(a^{-1}) = e.$$

Thus $aka^{-1} \in \ker \eta$ for all $a \in A$. Thus $\ker \eta \trianglelefteq A$. □

Remark. Now comes the climax of our present introduction to group theory which we have built up to: the First Isomorphism Theorem.

Theorem 2.24 (First Isomorphism Theorem)
Let $\eta : A \to B$ be a homomorphism between two groups. Then,

$$A/\ker\eta \cong \operatorname{im}\eta.$$

In particular, if η be an epimorphism, then

$$A/\ker\eta \cong B.$$

$$\begin{tikzcd}
A \arrow[r, "\eta"'] \arrow[d, "\varphi"] & B \\
A/\ker\eta \arrow[ur, "\psi"] &
\end{tikzcd}$$

Proof. Let $K = \ker\eta$. Define $\varphi : A \to A/K$ by $\varphi(a) = aK$. Define $\psi : A/K \to B$ by $\psi(aK) = \eta(a)$. If $a'K = aK$ then $a' = ak$ with $k \in K$ and

$$\eta(a') = \eta(ak) = \eta(a)\eta(k) = \eta(a).$$

Thus ψ is well-defined. $\operatorname{im}\psi = \operatorname{im}\eta$ and

$$\begin{aligned}
\psi(aK) = \psi(a'K) &\implies \eta(a) = \eta(a') \\
\text{and } e = \eta(a)^{-1}\eta(a) &= \eta(a)^{-1}\eta(a') \\
&= \eta(a^{-1})\eta(a') \\
&= \eta(a^{-1}a').
\end{aligned}$$

Thus, $e = \eta(e) = \eta(a^{-1}a') \implies e = a^{-1}a' \implies a = a'$. So ψ is injective. It is trivially a surjection onto $\operatorname{im}\psi = \operatorname{im}\eta$ thus ψ is an isomorphism between $A/\ker\eta$ and $\operatorname{im}\eta$. Thus,

$$A/\ker\eta \cong \operatorname{im}\eta$$

and in particular if η is an epimorphism then $\operatorname{im}\eta = B$ so

$$A/\ker\eta \cong B.$$

□

Example 2.7 1. $f : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ s.t. $f(i) = [i]$ is onto and

$$f(i + j) = [i + j] = [i] + [j] = f(i) + f(j).$$

Then, $\ker f = \{i \in \mathbb{Z} : f(i) = [0]\}$

$$= \{i \in \mathbb{Z} : i \equiv 0 \pmod{n}\} = \{nk : k \in \mathbb{Z}\} = n\mathbb{Z}.$$

Thus,

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

2. Let $f : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ s.t. $f(A) = \det(A)$. Then

$$f(AB) = \det(AB) = \det(A)\det(B) = f(A)f(B).$$

Let $r \in \mathbb{R}^*$ i.e. $r \neq 0$. Then

$$r = \det \begin{pmatrix} r & & \Large 0 \\ & 1 & \\ & & \ddots & \\ \Large 0 & & & 1 \end{pmatrix}_{n\times n} = \det(A) \neq 0,$$

for some $A \in \mathrm{GL}_n(\mathbb{R})$. Thus f is onto. $\ker f = \mathrm{SL}_n(\mathbb{R})$ $(\because f(A) = \det(A) = 1)$. Thus

$$\mathrm{GL}_n(\mathbb{R})/\,\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*.$$

§3 Group Exercises

Remark. All the theorems count as exercises too !

Problem 3.1. Show that $(\mathbb{Q}^+, \cdot) \cong (\mathbb{Z}[x], +)$.

Problem 3.2. Show that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff \gcd(m, n) = 1$.

Problem 3.3. Show that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Problem 3.4. Show that $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$.

Problem 3.5. Show that $(\mathbb{R}, +)/(\mathbb{Z}, +) \cong S^1$.

Problem 3.6. If $\eta : H \to K$ is a homomorphism between two groups, $a \in H : o(a) = n$, then show that $o(\eta(a)) \mid o(a)$.

Problem 3.7. Find all epimorphisms $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$.

Problem 3.8. Show that $\mathbb{Z} \ncong \mathbb{R}$.

Problem 3.9. Show that $S_3 \ncong \mathbb{Z}_6$, and for every proper subgroup A of S_3 there exists a proper subgroup B of $\mathbb{Z}_6$ such that $A \cong B$.

Problem 3.10. Show that every commutative group of order 6 is a cyclic group.

Problem 3.11 (Poincaré)**.** Let G be a group and H, K be subgroups of G of finite indices. Show that $H \cap K$ is of finite index.

Problem 3.12. Let G be the internal direct product of H and K. Then,

$$G \cong H \times K.$$

§3.1 Herstein "Topics in Algebra" Problems

Problem 3.13. Without using Lagrange's Theorem or any of its corollaries, show that if G is a finite group, then there exists a natural number N such that $a^N = e$ for all $a \in G$.

Problem 3.14. Let G be a group such that intersection of all its subgroups which are different from $\{e\}$ is a subgroup different from $\{e\}$. Prove that every element in G has finite order.

Problem 3.15. Suppose that H is a subgroup of G such that whenever $Ha \neq Hb$ then $aH \neq bH$. Prove that $gHg^{-1} \subseteq H$ for all $g \in G$.

Problem 3.16. Give an example of a group G and subgroup H such that the normaliser $N(H)$ and centraliser $C(H)$ are not the same. Is there any containment between $N(H)$ and $C(H)$?

Problem 3.17. If H is a subgroup of G then prove that

$$\bigcap_{x \in G} xHx^{-1} \trianglelefteq G.$$

Problem 3.18. If H is a subgroup of finite index in G, then show that there is only a finite number of distinct subgroups in G of the form aHa^{-1}.

§4 Rings

Remark. This is merely an introduction to rings, we will study ring theory in greater depth next semester.

§4.1 Definition and elementary properties

Definition 4.1 (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

   a) $a(b+c) = ab + ac$

   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 4.1

1. The **trivial ring** $R = \{0\}$.
2. The **ring of polynomials** $R[x]$ over a ring R defined as the set,

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

3. The ordinary integers $(\mathbb{Z}, +, \cdot)$, the integers modulo m, i.e., $(\mathbb{Z}_m, +, \cdot)$ 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 $f : [0, \infty) \to \mathbb{R}$ is integrable iff f is bounded and

   $$\int_0^\infty |\, f(x) \,| \ \mathrm{d}x = \lim_{t\to\infty} \int_0^t |\, f(x) \,| \ \mathrm{d}x < \infty.$$

   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 4.2

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

Definition 4.3

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

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

Theorem 4.1

Let R be a Boolean ring. Then, for all $x, y \in R$

1. $2x = 0$ and
2. $xy = yx$.

Proof.

1. Let $x \in R$, then $-x \in R$. So $x = x^2 = (-x)^2 = -x \implies 2x = 0$.
2. Let $x, y \in R$. Then $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$. Then, $xy = x + y - x - y - yx = -yx$. But $yx \in R$ so $yx = -yx$ and thus $xy = yx$.

□

Example 4.2

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.

§4.2 Integral domains, division rings and fields

Definition 4.4 (Integral domain)

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

Definition 4.5 (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 4.6 (Field)

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

Definition 4.7 (Characteristic)

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

Theorem 4.2

The following are equivalent:

1. R is an integral domain.
2. R is a commutative ring with identity $1 \neq 0$ such that the Cancellation Law holds for multiplication: $ab = ac \implies b = c \; \forall a, b, c \in R, \; a \neq 0$.

Proof. Let R be an integral domain. Then $a, b, c \in R, \; a \neq 0, \; ab = ac$. Then $a(b - c) = 0 \implies b - c = 0$ as R is an integral domain with $a \neq 0$. So $b = c$.

Conversely let R be a commutative ring with identity in which the Cancellation Law holds. Let $a, b \in R, \; a \neq 0, \; ab = 0$. Then $ab = 0 = a \cdot 0$ implies that $b = 0$. So R has no zero divisors, hence it is an integral domain. □

Theorem 4.3

Every field is an integral domain.

Proof. Let $\mathbb{F}$ be a field and $a, b \in \mathbb{F} : a \neq 0, \; ab = 0$. a is a unit in $\mathbb{F}$ so a^{-1} exists in $\mathbb{F}$. Thus $ab = 0 \implies b = 0$. Thus $\mathbb{F}$ is a commutative ring with identity $1 \neq 0$ and admitting no zero divisors. Thus $\mathbb{F}$ is an integral domain. □

Remark. Converse is not true: counterexample is $\mathbb{Z}$. However, any finite integral domain is a field.

Theorem 4.4

Any finite integral domain is a field.

Proof. Let R be a finite integral domain. Suppose $R = \{a_1, \ldots, a_n\}$. Let $a \in R \backslash \{0\}$, then consider $S = \{aa_1, \ldots, aa_n\}$. As R is closed under multiplication, $S \subseteq R$. If $aa_i = aa_j$ then $a_i = a_j$. So the elements of S are distinct. Thus $|S| = n = |R|, \; S \subseteq R \implies S = R$. As $1 \in R$ we have $1 = aa_j$ for some j implying that a_j is a unit and since this happens for every nonzero $a \in R$ we have that R is a field. □

§4.3 Subrings and subfields

Definition 4.8 (Subring)

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

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

Definition 4.9 (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 4.10 (Prime field)

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

§5 Ring Exercises

Exercise 5.1. (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) $(\mathbb{Z}\left[\sqrt{2}\right], +, \cdot)$, 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) $(\mathrm{GL}_n(\mathbb{R}), +, \cdot)$ 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
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b		
c	a			c
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 $\mathbb{H} = \{a_0 + a_1 i + a_2 j + a_3 k : a_r \in \mathbb{R},\ r = 0, 1, 2, 3\}$ such that $a_0 + a_1 i + a_2 j + a_3 k = b_0 + b_1 i + b_2 j + b_3 k \iff a_r = b_r$ 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 $\mathbb{Z}\left[\sqrt{2}\right]$ is closed under $+$ and $\cdot$. $+$ is associative and commutative as ordinary addition is associative and commutative, and $\cdot$ is associative as:

$$(x + y\sqrt{2})\Big((a + b\sqrt{2})(c + d\sqrt{2})\Big) = (xac + 2ybd) + (xad + ybc)\sqrt{2}$$

$$= \Big((x + y\sqrt{2})(a + b\sqrt{2})\Big)(c + d\sqrt{2}).$$

$0 = 0 + 0\sqrt{2}$ 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 $(\mathbb{Z}\left[\sqrt{2}\right], +)$ is an abelian group. Also $(\mathbb{Z}\left[\sqrt{2}\right], \cdot)$ 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, $(\mathbb{Z}\left[\sqrt{2}\right], +, \cdot)$ is a ring.

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

Thus, $(\mathrm{GL}_n(\mathbb{R}), +, \cdot)$ 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

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

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,

$$\ell \odot (m \oplus n)$$
$$= \ell \odot (m+n-1) = 2\ell + m + n - \ell m - \ell n - 1 = (\ell + m - \ell m) \oplus (\ell + n - \ell n)$$
$$= (\ell \odot m) \oplus (\ell \odot n).$$

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,

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

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 $R = \{f : \mathbb{R} \overset{\text{cont.}}{\longrightarrow} \mathbb{Z}\}$, but if $f : \mathbb{R} \to \mathbb{Z}$ is continuous then f must be constant. Thus, similar to the previous case, there exists the isomorphism $\phi : R \to \mathbb{Z}$ 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 $\phi : R \to 2\mathbb{Z}$ 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. $a \in R \implies \exists(-a) \in R : a + (-a) = 0 = (-a) + (-(-a))$

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

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 $M_2(\mathbb{R})$,

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

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

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

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

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

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

$$\begin{pmatrix} a_0 + a_1 i & a_2 + a_3 i \\ -a_2 + a_3 i & a_0 - a_1 i \end{pmatrix}.$$

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

$$\begin{pmatrix} a_0 + a_1 i & a_2 + a_3 i \\ -a_2 + a_3 i & a_0 - a_1 i \end{pmatrix} \begin{pmatrix} b_0 + b_1 i & b_2 + b_3 i \\ -b_2 + b_3 i & b_0 - b_1 i \end{pmatrix}.$$

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

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

so it is a Boolean ring.

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

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

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

$$-ar = -ra = -1$$

$$\implies (-a)(-r) = (-r)(-a) = 1$$

$$\implies -r = -a^{-1} \implies -(a)^{-1} = -a^{-1}.$$

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

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

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 Z_7 are $\{[1], \ldots, [6]\}$ 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 $R = \{a_1, \ldots, a_n\}$, $S = \{ba_1, \ldots, ba_n\}$. 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, taking $x = 1$ we have $x1 = 1x = 1$.

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,

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

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

Exercise 5.2. *Problems on subrings and subfields.*

1. Let

$$\mathbb{A} = \{\alpha \in \mathbb{C} : f(\alpha) = 0,\ f \in \mathbb{Q}[x],\ \deg(f) \in \mathbb{Z}_{\geq 0}\}$$

denote the set of **algebraic numbers** i.e. complex numbers satisfying some polynomial equation with rational coefficients. Show that $\mathbb{A}$ is a subfield of $\mathbb{C}$.

2. Prove that the characteristic of an integral domain is either prime or zero. In particular, prove that the characteristic of a field is either prime or zero.

3. Prove that the only prime fields are $\mathbb{Z}_p$ ($p = 1$ or prime) and $\mathbb{Q}$.

§6 Exam Papers

§6.1 2024

1. a) Define a *group*. Let $\mathbb{Z}_n$ be the set of all integers modulo some integer $n > 1$. Show that $\mathbb{Z}_n$ is not a group under multiplication whereas $\mathbb{Z}/n\mathbb{Z} = \{\bar{i} \in \mathbb{Z}_n : \gcd(n, \bar{i}) = 1\}$ is a group under multiplication.

   b) Let g be a group and $a, b \in G$ such that $a^2 = e$ and $ab^4a = b^7$ where e is the identity. Prove that $b^{33} = e$.

2. a) Define a *subgroup* of a group G. Show that $C(a) = \{g \in G : ag = ga\}$ is a subgroup of G for all $a \in G$.

   b) Prove that every infinite group has an infinite number of subgroups.

3. a) Let $\alpha, \beta, \gamma \in \mathrm{S}_8$ such that $\alpha = (1\ 2\ 3\ 8)$, $\beta = (3\ 5\ 8)$, and $\gamma = (1\ 3)(4\ 7)$. Let $x = \alpha^3\beta^{-2}\gamma$. Find the order of $x \in \mathrm{S}_8$.

   b) Define a *cyclic group*. Prove that every subgroup of a cyclic group is cyclic.

4. a) Let G be a group, H be a subgroup of G and $a, b \in G$. Prove that $aH = bH$ iff $a^{-1}b \in H$.

   b) Define a *normal subgroup* of a group G. Let H be a proper subgroup of G such that for all $x, y \in G \setminus H$, $xy \in H$. Prove that $H \trianglelefteq G$.

5. a) Define the *kernel* of a homomorphism (of groups). Let G be a group and $H \trianglelefteq G$. Then show that there exists an onto homomorphism $f : G \to G/H$ such that $\ker f = H$.

   b) Show that the mapping $f : (\mathbb{Z} \times \mathbb{Z}, +) \to (\mathbb{Z}, +)$ defined by $f((a, b)) = a - b$ is a homomorphism. Find $\ker f$.

6. a) Show that $(\mathbb{Q}, +)$ and $(\mathbb{Q}^*, \cdot)$ are not isomorphic groups.

   b) Show that every group is isomorphic to some subgroup of the group of all permutations of some set.

§6.2 2023

1. a) Define a *group*. Let G be a finite group and $a, b \in G$ such that $b \neq a$, $a^3 = e$, and $aba^{-1} = b^2$. Find the order of b.

   b) Define a *subgroup* of a group G. Let H be a subgroup of G. Show that for any $g \in G$,
   $$K = gHg^{-1} = \{ghg^{-1} : h \in H\}$$
   is a subgroup of G and $|K| = |H|$.

2. a) In S_7 let $\alpha(2\ 3\ 7\ 4)(1\ 5)\alpha^{-1} = (4\ 6\ 3\ 2)(5\ 7)$. Find α.

   b) Define the *alternating group* A_n. Let $H \trianglelefteq A_5$ such that H contains a $3-$*cycle*. Show that $H = A_5$.

3. a) Let G be a finite group of non-prime order $n > 1$. Show that G has a subgroup other than $\{e\}$ and G.

   b) Let G be a group with a finite number of subgroups. Show that G is finite.

4. a) Define a *cyclic group*. Prove that every subgroup of a cyclic group is cyclic.

   b) Let G be a nontrivial cyclic group. Show that $G \times G$ is not cyclic.

5. a) Let G be a group, H be a subgroup of G. Define the *left coset* aH of H in G for any $a \in G$. Prove that $aH = H \iff a \in H$ and $aH = bH \iff a^{-1}b \in H$ for any $a, b \in G$.

   b) Define a *normal subgroup* of a group G. Let H be a subgroup of G such that for all $aba^{-1}b^{-1} \in H$, $\forall a, b \in G$. Prove that $H \trianglelefteq G$.

6. a) Define the *homomorphism* of groups. Let G be a group and $H \trianglelefteq G$. Prove that there exists an onto homomorphism $\varphi : G \to G/H$ such that $H = \ker \varphi$.

   b) Show that $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$ for integer $n > 1$.