Outline of Group Theory

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

1 Groups

1. Binary operations. A binary operation on a nonempty set X is a map $\star\colon X \times X \to X$. We denote the image $\star(x, y)$ by $x \star y$ or xy if the binary operation is understood.

2. Examples.

   (a) The standard addition on $\mathbb{Z}$:

   $$+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \text{ defined by } +(m, n) := m + n.$$

   Similarly, the standard addition on $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, the set $M(n, \mathbb{R})$ of all square matrices of size n defines a binary operation the respective sets.

   (b) While the subtraction $-\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $-(m, n) := m - n$ is a binary operation on $\mathbb{Z}$, it is not a binary operation on $\mathbb{N}$

   (c) The map $(x, y) \mapsto x + y - 1$ defines a binary operation on $\mathbb{R}$.

   (d) The map $(x, y) \mapsto x + y + xy$ defines a binary operation on $\mathbb{R}$.

   (e) The map $(A, B) \mapsto A \cap B$ defines a binary operation on the power set $P(X)$ of a set X.

   (f) If S is any nonempty set, let $X := F(S, \mathbb{R})$ denote the set of all real valued functions on X. The map $(f, g) \mapsto f + g$ where $f + g \in F(S, \mathbb{R})$ is defined as $(f + g)(x) = f(x) + g(x)$ is a binary operation on X.

3. Groups: Definition.

4. Examples of groups.

   (1) The standard groups such as the additive group of integers, rational numbers, real numbers, complex numbers

   (2) The multiplicative group of the nonzero rational numbers, nonzero real numbers and nonzero complex numbers

   (3) The n-th roots of unity and all roots of unity

   (4) $S^1 := \{z \in \mathbb{C} : |z| = 1\}$ under multiplication of complex numbers.

(5) The set of matrices of a given type under addition

(6) Groups of nonsingular matrices such as $GL(n,\mathbb{R})$, $SL(n,\mathbb{R})$, $O(n,\mathbb{R})$. Give examples such as $\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}$, $\begin{pmatrix}a & -b\\ b & a\end{pmatrix}$, $(a,b)\neq(0,0)$.

(7) Functions from X to a group.

(8) $Sym(X)$.

(9) $ax+b$ group

(10) Let $G:=\{\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}, a\in\mathbb{R}^*, b\in\mathbb{R}\}$ is a group under matrix multiplication. (Do you observe any similarity between the binary operations of this group with the $ax+b$ group?)

(11) Dihedral Groups

(12) $\mathbb{Z}_n$ as the set of all congruences classes under a well-defined addition.

(13) $U_n:=\mathbb{Z}_n^*$.

(14) $\mathbb{R}$ under the operation $(x,y)\mapsto x+y-1$ as well as $(x,y)\mapsto x+y+xy$. The underlying principle. See also the next example.

(15) On $\mathbb{Q}^+$, define $a\star b:=ab/2$ where ab is the standard multiplication of two rational numbers.

(16) Klein's four group (as a set of matrices):
$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$.

(17) Quaternion group (as a set of matrices):
$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}, \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix}, \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix}$.
If we let $e=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $a=\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}$ and $b=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$, we have
$$a^4=e,\ b^2=a^2,\ \text{ and }\ b^{-1}ab=a^3.$$

(18) A matrix $A\in GL(2,\mathbb{R})$ is said to be *stochastic* if the coulmns add up to 1. Thus $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in GL(2,\mathbb{R})$ is stochastic if $a+c=1=b+d$. Show that the set of stochastic matrices from a group under matrix multiplication.

(19) Let G be a group and X a nonempty set. Let $H:=\{f\colon X\to G\}$. For $\alpha,\beta\in F(X,G)$ we define $\alpha\star\beta\equiv\alpha\beta\colon X\to G$ as $(\alpha\beta)(x):=\alpha(x)\beta(x)$. (Do you understand the right side?) With this binary operation, $F(X,G)$ becomes a group.

5. Basic Properties

(a) Uniqueness of the identity

(b) Uniqueness of the inverse

(c) Cancellation laws

(d) The only idempotent element is the identity

6. Generalized associativity and law of indices.

7. **Exercises:**

(1) Show that the complex numbers $\pm 1, \pm i$ form a group under multiplication. More generally, show that for any $n > 1$, the complex n-th roots of unit from a group under multiplication.

(2) Show that the maps $f_{ab}\colon x \mapsto ax + b$ $(a, b \in \mathbb{R}, a \neq 0)$ form a group under composition. Write down formulae for the product and inverse.

(3) Let $G := \{(x, y) \in \mathbb{R}^2 : ax + by = 0\}$ for a fixed $a, b \in \mathbb{R}$. Let $(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$. Show that this defines a binary operation on G and that G is a group under it.

(4) Consider the set of functions $f_1(x) = x$, $f_2(x) = \frac{1}{1-x}$, $f_3(x) = \frac{x-1}{x}$, $f_4(x) = \frac{1}{x}$, $f_5(x) = 1 - x$ and $f_6(x) = \frac{x}{x-1}$ defined on $\mathbb{R} \setminus \{0, 1\}$. Show that it forms a group under the composition of functions.

(5) Let G_i be a group, $i = 1, 2$. Let $G := G_1 \times G_2$ be the cartesian product. Define $(x_1, y_1) \star (x_2, y_2) := (x_1 x_2, y_1 y_2)$. Show that G is group under this binary operation.

(6) If $a_1, \ldots, a_n$ are elements of a group G, show that

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}.$$

Deduce that $(a^n)^{-1} = (a^{-1})^n$ for all $a \in G$ and $n \in \mathbb{N}$.

(7) Show that $G := \mathbb{R} \setminus \{-1\}$ is a group under the binary operation

$$a * b = a + b + ab, a, b \in G.$$

(8) Let G be a group and fix $c \in G$. Define a binary operation $a * b = acb$ for $a, b \in G$. Show that $(G, *)$ is a group.

(9) Let $n \in \mathbb{N}$. Let G be the set of all complex n-th roots of unity, that is, $C_n := \{e^{\frac{k2\pi i}{n}} : k \in \mathbb{Z}\}$. Show that G is a group under the usual multiplication of complex numbers.

(10) Show that the following statements are equivalent in a group G:
(i) G is abelian;
(ii) $(xy)^n = x^n y^n$ for all $x, y \in G$ and all $n \in \mathbb{Z}$;
(iii) $(xy)^n = x^n y^n$ for all $x, y \in G$ and for three consecutive integers n;
(iv) $(xy)^2 = x^2 y^2$ for all $x, y \in G$;
(v) $(xy)^{-1} = x^{-1} y^{-1}$ for all $x, y \in G$.

(11) Let G be a group which has a unique element g of order $n \geq 2$. Show that $n = 2$ and $gx = xg$ for all $x \in G$.

(12) Let G be a finite group. Show that the number of elements x such that $x^2 \neq 1$ is even. Hence conclude that if G is finite group of even order, then G has an element of order 2.

(13) Let a and b two non-commuting elements of a group. Show that the elements of the set $\{1, a, b, ab, ba\}$ are all distinct. Hence conclude that any non-abelian group has at least six elements.

(14) Let G be finite group. Show that for any $g \in G$, there exists $m \in \mathbb{N}$ such that $g^m = e$.

(15) Given $a, b, c \in G$, show that there exists a unique $x \in G$ such that $axb = c$.

(16) Let $a \in G$ be fixed. Show that the *left translation* $x \mapsto ax$ is a bijection of G onto itself. In particular, if $G = \{x_1, \ldots, x_n\}$, then $G = \{ax_1, \ldots, ax_n\}$.

(17) Let G be a group. Let $a, b \in G$ and $n \in \mathbb{N}$. Show that $(aba^{-1})^n = aba^{-1}$ iff $b = b^n$.

(18) Let G be a finite group and A, B subsets of G. Show that either $G = AB$ or $|G| \geq |A| + |B|$. *Hint:* Let $c \in G \setminus AB$. Consider the set $\{ca_1^{-1}, \ldots, ca_m^{-1}, b_1, \ldots, b_n\}$.

(19) Let A be a subset of a group G with $|A| > |G|/2$. Show that each element of G is a product of two elements of A.

(20) Let G be a group. Let K be a set and $f \colon G \to K$ be a bijection. For $y_1, y_2 \in K$, we define $y_1 \star y_2 := f(x_1 x_2)$ where $y_i = f(x_i)$, $i = 1, 2$. Show that $(K, \star)$ is a group.

(21) If a group G is generated by elements a, b and $ba = ab^k$, $a^n = 1$ show that every element of G can be written in the form $a^r b^s$ $(0 \leq r < n)$; show also that if $k \neq 1$, then $b^m = 1$ for some $m > 1$.

Hint: Any product $a^{r_1} b^{s_1} a^{r_2} b^{s_2} \cdots a^{r_m} b^{s_m}$ can be simplified by moving b past a, using the "relation" $ba = ab^k$ and reducing the exponent of a modulo n. Moreover, $ba^n = a^n b^{k^n}$, hence $b^m = 1$ for $m = k^n - 1$.

(22) Let G be a group. Let $a, b \in G$. Let $n \in \mathbb{N}$. Assume that we have the following *relations*: $a^n = e$, $b^2 = e$ and $aba = b$. Show that the set

$$\{e, a, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}\}$$

is the set of all possible finite products of a and b and that this set is a group under the induced binary operation.

This group of $2n$ elements is known as the n-th dihedral group and is denoted by D_{2n}.

(23) We now give a matrix representation of D_{2n}. Let $\zeta = e^{2\pi i/n}$ be a primitive n-th root of unity. Let $A = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(i) Prove that A has order n and that B has order 2.

(ii) Prove that $BAB = A^{-1}$.

(iii) Prove that the matrices of the form A^i and BA^i , for $0 \leq i < n$, form a multiplicative subgroup $G \leq GL(2, \mathbb{C})$.

(iv) Prove that each matrix in G has a unique expression of the form $B^i A^j$ where $i \in \{0, 1\}$ and $1 \leq j < n$.

(24) Let $G = \mathbb{R}^*$ Define $a \star b := |a|b$, the right side being the standard product of two real numbers. Is G a group?

(25) Let $(G, \cdot)$ be a group. Define a new binary operation on G as follows: $a \star b := b \cdot a$. Is $(G, \star)$ a group?

(26) Let G be a finite abelian group, say, $G = \{x_k : 1 \leq k \leq n\}$. Show that if $x = x_1 \cdots x_n$, then $x^2 = e$.

(27) Let G be a finite group. Assume that each element has a square root. That is, for each $a \in G$, we can find $x \in G$ such that $x^2 = a$. Show that each element has a unique square root. (*Hint:* This has nothing to do with group theory. Any map from a finite set to itself is one-one iff it is onto!

2 Subgroups

1. Let $f\colon X \to Y$ be any map. Let $S \subset X$. We then have a map $g\colon S \to Y$ defined by $g(a) = f(a)$ for $a \in A$. The map g is called the *restriction* of f to A. It is usually denoted by $f\,|_A$ or by f itself if there is no confusion.

2. Let H be a nonempty subset of G. When we restrict the binary operation on G to H (that is, the map $\star\colon G \times G \to G$ to $H \times H$), it may not be a binary operation as $\star(x, y) \notin H$ though $x, y \in H$.

3. A nonempty subset $H \subset G$ of a group is a *subgroup* of G if the binary operation on G induces a binary operation on H and H is a group under the induced binary operation.

4. Two subtle points to note:

   - If e_H denotes the identity of the element of the group H under the induced binary operation, then $e_H = e$, the identity element of G. This is true since $e_H^2 = e_H$ and the only element in G satisfying this relation is the identity element of G.
   - If $x \in H$ and $y \in H$ is such that $xy = yx = e_H (= e)$, then $y = x^{-1}$ by the uniqueness of the inverses **in** G.

5. If H is nonempty and finite with the property that $xy \in H$ for all $x, y \in H$, then H is a subgroup.

   If H is infinite this may not be true. Look at $\mathbb{N} \subset \mathbb{Z}$ under addition,

6. Let $H \subset G$ be a nonempty subset of a group. Then H is a subgroup of G iff for all $x, y \in H$ we have $xy \in H$ and $x^{-1} \in H$. This is equivalent to the condition that for all $x, y \in H$, the element $xy^{-1} \in H$.

7. Lots of examples of subgroups.

8. Complete description of subgroups of $\mathbb{Z}$; $m\mathbb{Z} \cap n\mathbb{Z}$, $m\mathbb{Z} + n\mathbb{Z}$.

9. Fix $A \subset X$ and look at $Sym(X; A)$ that leave A invariant.

10. All bijections that are identity outside a finite subset A, (A may vary).

    Let $f, g \in Sym(X; A)$. Let A and B be the finite subsets that correspond to f and g. Let $x \notin A \cup B$. Then $(f \circ g)(x) = f(g(x)) = f(x) = x$. Thus, $f \circ g$ is the identity outside the finite set $A \cup B$.

11. Intersection of a family of subgroups; smallest subgroup containing $S \subset G$. Its description when S is a singleton, all its elements commute etc.

12. **Exercises:**

    (1) Any subgroup of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ for a nonnegative integer m.

    (2) In $\mathbb{Z}$, we have $m\mathbb{Z} \subset d\mathbb{Z}$ iff d divides m.

    (3) Let $m, n \in \mathbb{N}$. Then the subgroup (?) set $(m\mathbb{Z}) \cap (n\mathbb{Z})$ is $\ell\mathbb{Z}$ where $\ell = \mathrm{lcm}(m, n)$.

(4) Let $m, n \in \mathbb{N}$. Then the set $m\mathbb{Z} + n\mathbb{Z}$ is $d\mathbb{Z}$ where $d = \gcd(m, n)$. In particular, we have the Bezout's identity:

$$d = \gcd(m, n) = am + bn \text{ for some } a, b \in \mathbb{Z}.$$

(5) This is perhaps the best place to introduce the group $U_n \equiv \mathbb{Z}_n^*$ of units modulo n. Details!

(6) Give examples of subgroups H, K of a group G such that $H \cup K$ is not a subgroup.

(7) If H, K are subgroups of a group, show that $H \cup K$ is not a subgroup unless one contains the other.

Hint: If neither contains the other, let $x \in H \setminus K$ and $y \in K \setminus H$. Then $xy \in H \cup K$ so that $xy \in H$ or $xy \in K$. In the first case, $x^{-1}(xy) = y \in H$ while in the second case $x = (xy)y^{-1} \in K$, a contradiction.

(8) Let H be a subgroup of G and $a \in G$. Show that $a \in H$ iff $aH = H = Ha$.

(9) If H is a subgroup of a group G, show that $HH = H$. Conversely, if H is a non-empty finite subset of G such that $HH = H$, then H is a subgroup of G. Give an example to show that the converse id false if H is infinite.

(10) Show that a finite group cannot be the union of two of its proper subgroups. Does this hold true if we replace two by three?

(11) Let G be an abelian group. Show that $H := \{a \in G : a^2 = 1\}$ is a subgroup of G.

(12) Let G be a group and $a, b, c \in G$. If a commutes with b and c, show that the set

$$C_a(G) := \{x \in G : ax = xa\}$$

is a subgroup of G. $C_a(G)$ is called the centralizer of a in G. Deduce that, for any subset X of G, the set $C_X(G) := \cap_{x \in X} C_x(G)$ is a subgroup.

(13) Let $Z(G) := \{g \in G : gx = xg \text{ for all } x \in G\}$. Show that $Z(G)$ is a subgroup of G. It is called the *centre* of G.

Can you get this as the intersection of a family of subgroups?

(14) Let $a \in G$. Show that $C_G(a)$, the centralizer of a in G is a subgroup of G and that $Z(G) \leq C_G(a)$.

(15) The *normalizer* $N_G(A)$ of any *set* A in a group G is defined as

$$N_G(A) := \{g \in G : gAg^{-1} = A\}.$$

Show that $N_G(A)$ is a subgroup of G. If A is subgroup of G, show that $A \leq N_G(A)$.

(16) If H is a proper subgroup of a group G, show that $G =< G \setminus H >$. *Hint:* Let $h \in H$. If $a \in G \setminus H$, consider $ah \notin H$. Hence $a^{-1}(ah) \in \langle G \setminus H \rangle$.

(17) Let G be abelian. Let $H, K \leq G$. Show that the set $HK := \{hk : h \in H, k \in K\}$ is a subgroup of G.

(18) Find all subgroups of a cyclic group.

(19) Find all subgroups of D_6, D_8 and D_{2n}.

(20) Let $H \leq G$. Define a relation $\sim$ on G by setting $x \sim y$ iff $xy^{-1} \in H$. Show that this defines an equivalence relation.

(21) Fix $n \in \mathbb{N}$, $n \geq 2$. Let $P_n := \{g^n : g \in G\}$. Can you think of a sufficient condition under which P_n is a subgroup? *Hint:* Abelian.

(22) Let $H, K \leq G$. Show that $HK := \{xy : x \in H, y \in K\}$ is a subgroup of G iff $HK = KH$.

(23) Let $H, K \leq G$ be finite. Show that $|HK| = \frac{|H||K|}{|H \cap K|}$. (Observe that HK need not be a subgroup.)

(24) Let (H_n) be a sequence of subgroups of a group G such that $H_n \subset H_{n+1}$ for each $n \in \mathbb{N}$. Show that $H := \cup_{n \in \mathbb{N}} H_n$ is a subgroup of G.

(25) If G is a group and $x, y \in G$, define their commutator to be $xyx^{-1}y^{-1}$, and define the commutator subgroup G to be the subgroup generated by all the commutators (the product of two commutators need not be a commutator).

(i) Prove that G' is normal subgroup of G.

(ii) Prove that G/G' is abelian.

(iii) If $f\colon G \to A$ is a homomorphism, where A is an abelian group, prove that $G' \leq \ker f$. Conversely, if $G' \leq \ker f$, prove that $\operatorname{Im} f$ is abelian.

(iv) If $G' \leq H \leq G$, prove that H is normal in G. (v) Let G^2 be subgroup generated by $\{x^2 : x \in G\}$. Show that $G' \leq G^2$.

3 Order of an element

(1) Order of an element. Let $g \in G$. Let $\langle g \rangle$ denote the smallest subgroup containing g. We have $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. If this subgroup is finite, we define the order of g by the equation

$$|g| \equiv \operatorname{ord}(g) := |\langle g \rangle|.$$

If $\langle g \rangle$ is not finite, we then say that g is of infinite order.

Observe that $\mathbb{Z}_g := \{n \in \mathbb{Z} : g^n = e\}$ is a subgroup of $\mathbb{Z}$. We have $\mathbb{Z}_g = n\mathbb{Z}$ if $\operatorname{ord}(g) = n$.

(2) Fix $a \in G$. Consider the map $f\colon \mathbb{Z} \to G$ defined by $f(n) = a^n$. It is a group homomorphism. Its kernel is the subgroup $\mathbb{Z}_a$, introduced in the last item. It is a subgroup of $\mathbb{Z}$ of the form $n\mathbb{Z}$, $n \geq 0$. If $n > 0$, then we observe that $\operatorname{ord}(a) = n$. The element a is of infinite order iff the kernel is trivial or what is the same, the homomorphism is one-one.

(3) Let $a \in G$ be of finite order, say n. When is $\langle a \rangle = \langle a^k \rangle$? It happens iff $\gcd(k, n) = 1$. Use Bezout's idendity.

(4) Let $\operatorname{ord}(a) = n$ and d divisor of n. The $\operatorname{ord}(x^d) = n/d$. More generally, for any positive integer k, $\operatorname{ord}(a^k) = n/\gcd(n, k)$.

Again, use Bezout's idendity to show that $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.

(5) Let $\operatorname{ord}(a) = n$. Then $a^r = a^s$ iff $r \equiv s\,(\,(\operatorname{mod} n))$. In particular, $a^k = a^r$ if r is the reminder of k when divided by n.

(6) Exercises (on Order of an element)

(1) Find the orders of the following elements in their respective groups: (a) [6] in $\mathbb{Z}_8$, (b) [26] in $\mathbb{Z}_{30}$.

(2) $\langle gag^{-1} \rangle = g \langle a \rangle g^{-1}$ and hence $\text{ord}(gag^{-1}) = \text{ord}(a)$. *Hint:* Observe that $(gag^{-1})^m = ga^m g^{-1}$.

(3) $\text{ord}(ab) = \text{ord}(ba)$. *Hint:* Are they conjugates?

(4) Let $\text{ord}(a) = m$, $\text{ord}(b) = n$. Assume that $\gcd(a, b) = 1$ and that $ab = ba$. Show that $\text{ord}(ab) = mn$.

(5) Find the possibilities of $\text{ord}(g)$ if
   (i) $g^3 = e = g^{20}$.
   (ii) $g^2 = g^6$ and $g^3 = g^{12}$.
   (iii) $g^{44} = e = g^{33}$ and $g^2 \neq e$.

(6) Let $a, b \in G$ be such that $\text{ord}(a) = 12$ and $\text{ord}(b) = 33$. Assume that $\langle a \rangle \cap \langle b \rangle$ is nontrivial. Show that $a^4 = b^{11}$.

(7) Let $\text{ord}(a) = m$, $\text{ord}(b) = n$. Assume that $\gcd(a, b) = d$ and that $ab = ba$. Show that then are exists an element c such that $\text{ord}(c) = mn/d$. *Hint:* Let $x = a^d$. Observe that $\text{ord}(c) = m/d$ is co-prime to n.

(8) Let $H \leq G$. Assume that $\text{ord}(g) = n$ and $g^m \in H$. If $\gcd(m, n) = 1$, show that $g \in H$.

(9) Let $g \in G$ be the unique element of order n. Show that $gx = xg$ for all $x \in G$. *Hint:* To say $xg = gx$ is the same as saying $xgx^{-1} = x$.

(10) Let $|G| = n$ and $k \in \mathbb{N}$ be such that $\gcd(n, k) = 1$. Fix $a \in G$. Show that there exists a unique solution to the equation $x^k = a$. *Hint:* Bezout's identity and Lagrange's theorem.

(11) Let G be a finite group and $n > 2$. Show that the number of elements of order n is even.

(12) Groups of even order have an odd number of elements of order 2.

(13) Consider $([1], [1]) \in \mathbb{Z}_2 \times \mathbb{Z}_3$. What is its order? Can you generalize this?

(14) Let $m, n \in \mathbb{N}$ be relatively prime. Show that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

(15) Let $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. Find the orders of A, B and AB.

(16) Let $H \leq G$ be a subgroup of index 2. Then
   (i) For any $x \in G$, we have $x^2 \in H$.
   (ii) H is normal in G.

(17) A_4 does not have a subgroup of order 6.
   If one such H exists, its index is 2 and hence for any $\sigma \in S_4$, we have $\sigma^2 \in A_4$. There are eight ($\frac{4 \times 3 \times 2}{3}$) 3-cycles in S_4. If α is one of them, then $\alpha = \alpha^4 = (\alpha^2)^2 \in A_4$.

(18) Find the centre of $GL(2, \mathbb{R})$. *Hint:* Any element has to commute with $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and with $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.
   A general proof using the permutations may be indicated for $GL(n, \mathbb{R})$.

(a) Lots of examples to show the power of the concept in settling the existence non-existence of isomorphisms, homomorphisms between groups.

4 Lagrange's Theorem

(1) Recall that if $1 < n \in \mathbb{N}$, we defined an equivalence relation by setting $a \equiv b$ if $b-a = -a+b$ is divisible by n. In terms of the subgroup $n\mathbb{Z}$, $a \equiv b$ iff $-a+b \in n\mathbb{Z}$.

(2) We mimic the congruence relation if we are given a subgroup $H \leq G$. We say that $a \equiv b$ if $a^{-1}b \in H$. This defines an equivalence relation on G.

(3) The equivalence class $[a]$ of $a \in G$ is the *left coset* $aH := \{ah : h \in H\}$.

(4) The map $h \mapsto ah$ is a bijection from H onto aH.

(5) Let G be finite. Let the equivalence classes be eH, $a_1H, \ldots, a_{k-1}H$. Since their union is disjoint and all of G, we arrive at Lagrange's theorem: $|G| = |H| \times k$. k is called the index of H in G and is denoted by $[G : H]$.

(6) If $H \leq G$, the set of left cosets of H in G is denoted by G/H.

(7) Let G be finite. Then $\mathrm{ord}(G)$ is a divisor of $|G|$.

(8) If $|G| = n$, then $g^n = e$ for any $g \in G$.

(9) Let G be finite. If $H \leq G$, then $|G/H| = |G|/|H|$.

(10) Exercises:

  (1) Every group of order p is cyclic and is isomorphic to $\mathbb{Z}_p$.

  (2) Let $|G| = 4$. Show that G is abelian. *Hint:* If G is not cyclic, what can you say about $\mathrm{ord}(x)$ for $x \in G$?

  (3) Every group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

  (4) If G is a group which has only $\{e\}$ and G as its subgroups, then G is isomorphic to $\mathbb{Z}_p$ for some prime p.

  (5) Let $a \in G$ be of order 30. What is the index of $\langle a^4 \rangle$ in $\langle a \rangle$?

  (6) Let $H \leq K \leq G$. Show that $[G : H] = [G : K] \times [K : H]$.

  (7) Let $H \leq G$ and $K \leq G$. Assume that $\gcd(|H|, |K|) = 1$. Show that $H \cap K = \{e\}$.

  (8) Let $H \leq G$ and $K \leq G$. Assume that there exist distinct primes p and q such that $[G : H] = p$ and $[G : K] = q$. Show that pq divides $[G : H \cap K]$.

  (9) Let $H \leq G$ be proper. Show that $\langle G \setminus H \rangle = G$. *Hint:* Enough to show H is captured. Look at the coset decomposition.

5 Normal subgroups

(1) We say that a subgroup $H \leq G$ is *normal* in G if all $g \in G$ and $h \in H$, we have $ghg^{-1} \in H$. We denote this by $H \trianglelefteq G$.

(2) The following are equivalent for a subgroup $H \leq G$:
  (i) $H \trianglelefteq G$.
  (ii) For each $a \in G$, we have $aHa^{-1} \subset H$.
  (iii) For each $a \in G$, we have $aHa^{-1} = H$.
  (iv) For each $a \in G$, we have $aH = Ha$.

(3) Exercises:

  (1) Let $H \leq Z(G)$. Show that H is normal in G.

(2) Any subgroup of an abelian group is normal.

(3) Any subgroup of the quaternion group $\mathbf{Q}$ is normal.
The only significant case is when $|H| = 2$. The only element of order 2 in $\mathbf{Q}$ is -1 which lies in the centre.

(4) Let $[G : H] = 2$. Prove that H is normal in G.

(5) Let H be the unique subgroup of order $|H|$. Prove that $H \trianglelefteq G$.

(6) Let G be finite. Assume that $H \leq G$ is the only subgroup of index $[G : H]$. Prove that $H \trianglelefteq G$.

(7) Let $N \trianglelefteq G$ be cyclic. Let $H \leq N$. Show that $H \trianglelefteq G$.

(8) Show that $\ker f$ of any homomorphism is a normal subgroup of the domain.

(9) Show that $A_n \trianglelefteq S_n$.

(10) Show that $SL(n, \mathbb{R}) \trianglelefteq GL(n, \mathbb{R})$.

(11) Show that $S_F(X) \trianglelefteq S(X)$. (Recall that $S_F(X)$ consists of bijections of X that move only finite subsets of X.) Give Ref!

(12) The commutator subgroup G' of G is normal. In fact, any subgroup containing the commutator subgroup is normal.

(13) Let $N \trianglelefteq G$ and $N \cap G' = \{e\}$. Show that $N \subset G'$.

(14) Let $N \trianglelefteq G$ and $H \leq G$. Show that $NH = HN$ is a subgroup of G. Show further that it is normal if $H \trianglelefteq G$.

(15) With the notation of the last item, show that $H \cap N \trianglelefteq H$.

(16) Lt $f\colon G \to H$ be an onto homomorphism. If $N \trianglelefteq G$, show that $f(N) \trianglelefteq H$.

(17) Let $f\colon G \to H$ be an onto homomorphism. Show that a subgroup K such that $\ker f \leq K \leq G$ is normal in G iff $f(K)$ is normal in H.

(18) The diagonal subgroup $\Delta(G) := \{(g, g) : g \in G\}$ is normal in G iff G is abelian.

(19) Let G be a group and $N \in \mathbb{N}$. Let $H := \{g^N : g \in G\}$. Show that H is a subgroup iff it is a normal subgroup.

(20) Prove that a subgroup $N \leq G$ is normal iff for all $x, y \in G$ we have $xy \in N$ iff $yx \in \mathbb{N}$.

(21) Let $H \trianglelefteq G$ and $K \trianglelefteq G$. Assume that $H \cap K = \{e\}$. Show that for $x \in H$ and $y \in K$, we have $xy = yx$.

(22) Prove that the intersection of normal subgroups is again a normal subgroup.

(23) Let H be a subgroup of order m in a group G. Prove that the intersection of all subgroups of order m is a normal subgroup of G.

(24) The set of inner automorphisms of a group is a normal subgroup of the group of automorphisms of G.

(25) A subgroup $H \leq G$ is normal iff the product of any two left cosets is again a left coset.

(26) Let $H \trianglelefteq G$ and $|H| = 2$. Show that $H \leq Z(G)$.

(27) Show that $G \times \{e\} \trianglelefteq G \times H$.

(28) True or false? $N \trianglelefteq G$ and $x \in N$, $g \in G \implies gxg^{-1} = x$.

(29) Assume that every subgroup of G is normal. Let $x, y \in G$ and $\gcd(\mathrm{ord}(x), \mathrm{ord}(y)) = 1$. Show that $xy = yx$.

(30)

13. Centre, centralizer and normalizer. Normal Subgroups in S_5 and A_5; centres of S_n, A_n, D_{2n} and $GL(n, \mathbb{R})$.

6 Cyclic Groups

1. **Cyclic Groups.** We say that a group G is cyclic if there exists $a \in G$ such that $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

2. Examples of cyclic groups.

   (a) $\mathbb{Z}$.

   (b) $\mathbb{Z}_n$.

   In fact, these are the only cyclic groups up to isomorphism. Explain the statement. For instance, the cyclic n-th roots of unity is isomorphic to $\mathbb{Z}_n$.

3. Subgroups of cyclic groups. The following theorem gives complete information on this issue.

   Theorem 1. *Let G be a cyclic group.*
   (1) Let G be an infinite cyclic group, say, $G = \langle a \rangle$. Then $G = \langle x \rangle$ iff $x \in \{a, a^{-1}\}$. Any of its subgroup H is of the form $H = \langle a^n \rangle$ where n is the least non-negative integer such that $a^n \in H$.
   (2) Let $G = \langle a \rangle$ be finite, say, of order n. Then
   (i) $G = \langle a^k \rangle$ iff $\gcd(k, n) = 1$.
   (ii) For each divisor d of n, there exists a unique subgroup $H_d = \langle a^{n/d} \rangle$. There are the only subgroups of G.

4. A group G of order n is cyclic if and only if, for each divisor d of n, there is at most one (cyclic?) subgroup of order d.

   One way is already seen.

   Conversely, define a relation on a group G by ab if $\langle a \rangle = \langle b \rangle$. It is easy to see that this is an equivalence relation and that the equivalence class $[a]$ of $a \in G$ consists of all the generators of $C = \langle a \rangle$. Thus, we denote $[a]$ by $\mathrm{Gen}(C)$, and

   $$G = \cup_{C \text{ cyclic}} \mathrm{Gen}(C).$$

   Hence, $n = |G| = \sum_C |\mathrm{Gen}(C)|$, where the sum is over all the cyclic subgroups of G. We know that $|\mathrm{Gen}(C)| = \varphi(|C|)$. By hypothesis, G has at most one (cyclic) subgroup of any order, so that

   $$n = \sum_C |\mathrm{Gen}(C)| \leq \sum_{d|n} \varphi(d) = n.$$

   Therefore, for each divisor d of n, there must be a cyclic subgroup C of order d contributing $\varphi(d)$ to $\sum_C |\mathrm{Gen}(C)|$.

5. Exercises on Cyclic Groups.

   (1) Show that $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

(2) Show that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

(3) Let $|G| = 20$. Assume that there exist 3 elements of order 4 in G. Can G be cyclic? What if G has only two elements of order 4?

(4) Show that an abelian group of square-free order (i.e. of order not divisible by a square) is cyclic.

Hint: Pick an element of largest order r. If $|G| > r$, there is an element b of prime order p not dividing r but ab has order $pr > r$, a contradiction.

(5) Let H be the subgroup $\langle [28], [88] \rangle$ in $\mathbb{Z}_{154}$. Find k such that $H = \langle [k] \rangle$.

(6) Euler's φ-function. Group theoretic proof of $\sum_{d|n} \varphi(d) = n$. N&S for a finite group to be cyclic.

7 Homomorphisms

(1) Homomorphisms: Definition and examples; Fix $a \in G$, consider $n \mapsto a^n$. Standard properties. All homomorphisms of $\mathbb{Z}$ to itself.

(2) Let G and H be groups. A map $f\colon G \to H$ is said to be a *homomorphism* if for all $x_1, x_2 \in G$, we have $f(x_1x_2) = f(x_1)f(x_2)$. Do you understand what is the meaning of x_1x_2 on the left side and that of $f(x_1)f(x_2)$ on the right side?

(3) Any homomorphism of $\mathbb{Z}$ to itself is of the form $f(x) = mx$ for some $m \in \mathbb{Z}$.

(4) Projection map $\pi_i\colon G_1 \times G_2 \to G_i$, given by $\pi_1(x_1, x_2) = x_1$ etc. Can you think of a group homomorphism from G_i to $G_1 \times G_2$?

(5) The map $f\colon \mathbb{Z} \to \mathbb{Z}_n$ given by $f(k) = [k]$.

(6) Let $p, q \in \mathbb{N}$ with $\gcd(p, q) = 1$. The map $f\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_p \times \mathbb{Z}_q$ defined by $f(m, n) := ([m], [n])$ where $[m]$ is the congruence class of m modulo p etc.

(7) The map $f\colon GL(n, \mathbb{R}) \to \mathbb{R}^*$ defined by $f(X) = \det(X)$.

(8) The map $f\colon M(n, \mathbb{R}) \to M(n, \mathbb{R})$ defined by $f(A) := A + A^t$ where A^t is the tanspose of A.

(9) Fix $a \in G$. The map $f\colon G \to G$ defined by $f(x) := axa^{-1}$.

(10) Consider the group $\mathbb{R}$ with the binary operation $\star : (x, y) \mapsto x + y - 1$. Show that the map $f\colon (\mathbb{R}, +) \to (\mathbb{R}, \star)$ defined by $f(s) = s + 1$ is an isomorphism.

(11) Can you think of an analogous homomorphism from $(\mathbb{R}^*, \cdot)$ to $(\mathbb{R} \setminus \{-1\}), \star)$ where $\star(a, b) := a + b + ab$?

(12) The map $f\colon \mathbb{C}^* \to \mathbb{C}^*$ defined by $f(z) = z^n$, $n \in \mathbb{Z}$ fixed.

(13) The map $f\colon \mathbb{C}^* \to \mathbb{R}^+$ defined by $f(z) = |z|$.

(14) The map $f\colon \mathbb{C}^* \to S^1$ defined by $f(z) := \frac{z}{|z|}$.

(15) The map $f\colon \mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = e^x$.

(16) Exerices:

  (1) Show that a group G is abelian iff the map $f(x) = x^{-1}$ is a homomorphism.

  (2) Show that a group G is abelian iff the map $f(x) = x^2$ is a homomorphism.

  (3) Consider the map $x \mapsto 3x$ from $(\mathbb{Q}^+, \cdot)$ to itself. Is it an isomorphism? Is it an isomorphism of $(\mathbb{Q}, +)$?

(4) Is $(\mathbb{Q}, +)$ isomorphic to $\mathbb{Q}^+, \cdot)$?

(5) Let $f, g\colon G \to K$ be group homomorphisms. Let $H := \{x \in G : f(x) = g(x)\}$. What can you say about H?

(6) Let $f\colon \mathbb{Z}_{29} \to G$ be a group homomorphism such that f is not one-one. Determine f.

(7) Let G be a finite group such that there exists an *onto* homomorphism of $f\colon \mathbb{Z} \to \mathbb{Z}_n$. What can you say about $|G|$?

(8) Let G be a finite group such that $\mathbb{Z}_20$ and $\mathbb{Z}_12$ are $f(G)$ and $g(G)$ for homomorphisms f and g. What can you say about $|G|$?

(9) Let $f\colon \mathbb{Z}_{21} \to \mathbb{Z}_7$ be onto. Determine $\ker(f)$.

(10) Find all homomorphisms of $\mathbb{Z}_n$ to itself.

(11) Fix $m, n \in \mathbb{N}$. Consider the map $f\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $f(x, y) = mx + ny$. Identify the image and kernel of f.

(12) Let $m, n \in \mathbb{N}$. Define $f\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by setting $f([k]) = ([k], [k])$. (Do you understand that $[k]$ has different meanings in this definition?) Show that this is well-defined and that it is an isomorphism iff $\gcd(m, n) = 1$.

(13) Deduce from the last exercise that if $\gcd(m, n) = 1$, we have $\varphi(mn) = \varphi(m)\varphi(n)$.

(14) Let $f\colon G \to K$ be a homomorphism and $a \in G$. Show that $\mathrm{ord}(f(a))$ divides $\mathrm{ord}(a)$. (Assume that a is of finite order.)

(15) Find all homomorphisms from $\mathbb{Z}_6$ to $\mathbb{Z}_{13}$. Can you generalize your observation?

(16) Let G be abelian. Fix $n \in \mathbb{N}$. Show that $f\colon G \to G$ defined by $f(g) = g^n$ is a homomorphism.

(17) With the notation of the last exercise, let $|G| = m$. Show that f is an automorphism iff $\gcd(m, n) = 1$.

(18) Let $f\colon G \to G$ be an automorphism. Assume that the only fixed point of f (that is, an element $x \in G$ sucht hat $f(x) = x$) is the identity. Show that $G = \{xf(x^{-1}) : x \in G\}$.

(19) Let $f\colon G \to G$ be an automorphism. Assume that the only fixed point of f (that is, an element $x \in G$ sucht hat $f(x) = x$) is the identity. Assume further that $f \circ f$ is the identity. Prove that the group G is abelian. *Hint:* Enough to show that $f(xyx^{-1}y^{-1}) = xyx^{-1}y^{-1}$.

(20) Let $f\colon G \to H$ be a homomorphism. Assume that $\ker f \leq K \leq G$. Prove that $K \trianglelefteq G$.

(21) Let H be a simple group, that is, the only normal subgroups of H are $\{e\}$ and H. Let $f\colon G \to H$ a homomorphism. Show that either f is trivia or f is one-one.

(17) Use of isomorphisms:

i. Let $G := \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R}, a^2 + b^2 \neq 0\}$. Show that G is a group under matrix multiplication and that it is isomorphic to $\mathbb{C}^*$.

ii. Let $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, with $a^2 + b^2 \neq 0$. Let $n \in \mathbb{N}$. Show that there exists a matrix $B = \begin{pmatrix} u & -v \\ v & u \end{pmatrix}$ such that $B^n = A$.

iii. Show that the $ax+b$ group and the stochastic group (on page 2) are isomorphic.
Hint: If A is stochastic, let $f(A) := BAB^{-1}$ where $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

8 Symmetric Groups

Cycle structure, transposition, sign of a permutation, alternating groups.

(1) Let X be any nonempty set. The set of bijections of X is a group under composition of maps. It is called the symmetric group on X,

(2) If X is a finite set, say, $X = \{1, \ldots, n\}$, the group $S(X)$ is denoted by S_n. We have $|S_n| = n!$

(3) If $|X| \geq 3$, then $S(X)$ is not abelian. For, if x, y, z are distinct elements of X, consider $\sigma \in S(X)$ defined by $\sigma(x) = y$, $\sigma(y) = x$ and $\sigma(x) = x$ for $x \notin \{x, y\}$. Similarly, define $\tau(y) = z$, $\tau(z) = y$ and $\tau(x) = x$ for $x \neq y, z$. Then $\sigma \circ \tau(x) = \sigma(x) = y$ whereas $\tau \circ \sigma(x) = \tau(y) = z$.

(4) If $\sigma \in S_n$, we denote it as a $2 \times n$ matrix where $a_{1i} = i$ and and $a_{2i} = \sigma(i)$:

$$\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

(5) Fix $\sigma \in S(X)$. Let $H := \langle \sigma \rangle$. We have the natural action of H on X. We have an oribit decomposition of X under H. Let $X = \sqcup X_i$ be the disjoint union of the orbits. Then σ maps each X_i to itself. If we dfine σ_i to be restriction of σ to X_i we can reconstruct σ from σ_i's.

It is expedient to consider $\sigma_i \in S(X)$ by letting $\sigma_i(x) = x$ if $x \notin X_i$.

If $S(X) = S_n$, we then have the cycle decomposition of σ as $\sigma = \sigma_1 \cdots \sigma_k$. (The order does not matter. See the next item.) Give a few examples os that students learn how to do this.

(6) Let $\alpha, \beta \in S(X)$. Assume that there exist disjoint subsets $A, B \subset X$ such that $\alpha(x) = x$ for $x \notin A$ and $\beta(x) = x$ for $x \notin B$. (Note that α maps A to itself etc.) Then $\alpha \circ \beta = \beta \circ \alpha$.

(7) Keep the notation of the last item. Then α is called a *cycle*. Give examples of cycles in S_n. What the last item says: Disjoint cycles commute.

(8) In S_n, a cycle is denoted by $(i_1, i_2, \ldots, i_r)$. This is the bijection which maps $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $i_k \mapsto i_1$ and on the rest it is the identity.It is said to be of length k.

(9) A $\sigma \in S(X)$ said to be a *transposition* if it is a cycle there exist two distinct elements x, y such that $\sigma(x) = y$, $\sigma(y) = x$ and $\sigma(z) = z$ for $z \neq x, y$. Thus it is a cycle of length 2.

(10) *Any $\sigma \in S_n$ is a product/composition of transpositions.*

Since σ is a product of cycles, enough to show that any cycle is a product of transpositions:

$$(i_1\ i_2\ \ldots, i_k) = (i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_2).$$

(11) Consider $P := \prod_{i<j}^{n}(x_i - x_j)$. If $\sigma \in S_n$, let $\sigma \cdot P := \prod_{i<j}(x_{\sigma(i)} = x_{\sigma(j)})$. Then $\sigma \cdot P = \varepsilon P$ where $\varepsilon \in \{\pm 1\}$. ε defined by this equation is called the *sign* of the permutation σ and denoted by $\varepsilon(\sigma)$ or $\text{sign}(\sigma)$.

Noe that if σ is a transposition, then $\varepsilon(\sigma) = -1$.

(12) The following are true:
(i) $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.
(ii) $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.
(iii) The map $\varepsilon\colon S_n \to \{\pm 1\}$ is a group homomorphism.

(13) The kernel of the homormorphism is a normal subgroup called the alternating group and is denoted by A_n. Note that $|A_n| = n!/2$.

(14) If σ is written as a product of k and ℓ transpositions, then $k \equiv \ell(\,(\mathrm{mod}\, 2))$.

(15) Observe that if σ is a k-cycle, then $\varepsilon(\sigma) = k - 1$.

(16) If σ is a product of r-cycles *including* the cycles of length 1, then $\varepsilon(\sigma) = (-1)^{n-r}$.

(17) Simplicity of A_n, $n \geq 5$.

i. If $n \geq 3$, the group A_n is generated by 3 cycles.
Since any 3-cycle is even, it lie sin A_n. Any element of A_n is a product of an even number of transpositions. Observe the following:

$$(a, b)(c, d) = (adb)(adc) \tag{1}$$

$$(ab)(ac) = (acb). \tag{2}$$

ii. A_1, A_2 and A_4 are not simple. A_3 is simple.

iii. Let N be a proper nontrivial normal subgroup of A_n, $n \geq 5$. Then N cannot have 3-cycles.
Let $(abc) \in N$. Let (rst) be another 3-cycle. Let $\sigma \in S_n$ be such that σ maps a, b, c to r, s, t in respective order. Then $\sigma(abc)\sigma^{-1} = (rst)$. It may happen that $\sigma \notin A_n$. Since $n \geq 5$, we can take $\tau = \sigma(u, v)$ for $u, v \notin \{a, b, c\}$. Then $\tau \in A_n$ and we have $\tau(abc)\tau^{-1} = (rst)$. Thus, if N has one 3-cycle, it has all three cycles. In view of the last item, we conclude that $N = A_n$, a contradiction.

iv. Let N be a proper nontrivial normal subgroup of A_n, $n \geq 5$. Then N cannot any cycle of length greater than or equal to 4 in its cycle decomposition.
If it does, we shall show that it contains a 3-cycle. Let

$$\sigma = (abcd\ldots)\cdots \in N$$

Then N contains its A_n-conjugate

$$\tau = (abc)\sigma(abc)^{-1} = (bcad\ldots)\cdots$$

Hence $\tau\sigma^{-1} = (abd) \in N$. But then by an earlier observation, $N = A_n$. Hence we conclude that the elements in N will have cycle decomposition of cycle lengths at most 3.

v. Keep the notation as above. We claim that N cannot have an element with two 3-cycles in its cycle decomposition.
For, if $\mathbb{N} \ni \sigma = (abc)(rst)\cdots$, then the A_n-conjugate

$$\tau = (rst)\sigma(rst)^{-1} = (abr)(cts)\cdots .$$

Hence $\sigma\tau = (acrbs)\cdots$. But this was seen to be impossible. We are therefore led to conclude that N contains elements which are products of even number of transpositions.

vi. Let $\sigma \in N$ be of the form $\sigma = (ab)(rs)$. Choose c different from the 4 elements involved in σ. Then

$$\tau = (acb)\sigma(acb)^{-1} = (ac)(rs) \in N.$$

Hence $\sigma\tau = (acb) \in N$, a contradiction.
So, if $\sigma \in N$, in its cycle decomposition, we must have at least 4 transpositions.
Let $\sigma = (a_1b_1)(a_2b_2)(a_3b_3)(a_4b_4)\cdots$. Now,

$$\tau = (a_3b_2)(a_2b_1)\sigma(a_2b_1)(a_3b_2) = (a_1a_2)(a_3b_1)(b_2b_3)(a_4b_4)\cdots \in N.$$

The element $\sigma\tau = (a_1b_2a_3)(a_2b_1b_3) \in \mathbb{N}$, a contradiction.

vii. A_n is simple if $n \geq 5$.
Follows from the last few items.

(18) Exercises:

(1) Find all subgroups of S_4.
Answer: S_4, A_4, V_4 Klein's four group (four times), three subgroups of order 8 obtained by extending V by a transposition, 3 cyclic groups of order 4 generated by a 4-cycle, 4 subgroups of order 6, arising as stabilizer of a symbol.

(2) Show that in S_n a cycle of length n commutes only with its powers. Does this still hold for a cycle of length $n-1$? Show that S_n has trivial center for $n \geq 3$ and A_n has trivial center for $n \geq 4$.
Hint: If we conjugate $\alpha = (1\,2\ldots n)$ by σ, then we get $(\sigma 1\ \ldots \sigma n)$. This is same as α iff is is a cyclic permutation of $(1\,2\ \ldots n)$, that is, σ is a power of α.
The same holds true for $\beta = (1\,2\ \ldots n-1)$, since if $\beta^\sigma = \beta$, then $\sigma(n) = n$. Thus effectively, σ is a permutation of the first $n-1$ symbols.
For $n > 3$, S_n has two n cycles, and hence its center is 1. The same holds for $n = 3$ as can be seen by direct verification.
For $n > 4$, if n is even, A_n contains two $(n-1)$ cycles not powers of each other. When n is odd, it contains two n cycles not powers of each other. A_4 has trivial center by direct verification.

(3) Find $\alpha^{-1}\beta^{-1}\alpha\beta$ in the following cases: (i) $\alpha = (1\,2\,3), \beta = (1\,4\,5)$, (ii) $\alpha = (1\,2\,3\,4), \beta = (1\,3\,5)$ and (iii) $\alpha = (1\,2\,3), \beta = (4\,5\,6)$.
Answer: (i) $(1\,4\,2)$, (ii) $(1\,3\,5\,4\,2)$, (iii) 1.

(4) Show that the elements $1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)$ form a subgroup of A_4. Any group isomorphic to this subgroup is called Klein's four group.

(5) Show that S_n is generated by $(1\,2), (2\,3), \ldots, (n-1\,n)$.
Answer:

$$(1\,2\ldots i) = (i-1\,i)(i-2\,i-1)\cdots(1\,2)$$
$$(i\,i+k+1) = (1\,2\ldots i+k)^k(i+k\,i+k+1)(1\,2\ldots i+k)^{-k}.$$

(6) Show that S_n is generated by $(1\,2\,3\ldots n)$ and $(1\,2)$.
Hint: $(i+1\,i+2) = (1\,2\ldots n)^{-i}(1\,2)(1\,2\ldots n)^i$; now use the last exercise.

(7) Show that A_n is denoted by $(1\,2\,3)$ and $(1\,2\,3\ldots n)$ or by $(1\,2\,3)$ and $(2\,3\ldots n)$ according as whether n is odd or even.
Hint: $(i+1\,i+2\,i+3) = (1\,2\ldots n)^{-i}(1\,2\,3)(1\,2\ldots n)^i$.

(8) Show that an n-cycle $(1\,2\,3\ldots n)$ can be expressed as a product of $n-1$ cycles but no fewer.
Hint: $(1\,2\ldots n) = (1\,2)(1\,3)\cdots(1\,n)$. Let $t_1\cdots t_k$be a representation as a product of k transpositions ($n > 2$ say). Since $(1\,2\ldots n)$ interchanges no two symbols, one of the symbols in t_k must occur elsewhere, so t_k introduces only one new symbol; likewise for $t_{k-1},\ldots,t_2$, while t_1 introduces two symbols. But all symbols are moved, so $k+1 \geq n$, i.e., $k \geq n-1$.

(9) Show that every finite group is isomorphic to a subgroup of A_n for some n.
Hint: Let $\varphi\colon G \to Sym(X)$ be an one-one homomorphism. Then the map $x \mapsto (\varphi(x),1)\cdot(\varphi(x),2)$ on $X\times 2$ is an injective homomorphism into even permutations.

(10) Let G be subgroup of S_n not contained in A_n. Show that exactly half the permutations in G are even.
Hint: Write $A = G\cap A_n$. If $x \in G\setminus A_n$, then $G = A\cap xA$.

(11) Show that any group of order $4n+2$ has a subgroup of index 2. *Hint:* Use the last exercise.
Answer:

9 Classes of Groups

(a) Cyclic groups: Subgroups, generators, Euler's φ-function. Group theoretic proof of $\sum_{d|n}\varphi(d) = n$. N&S for a finite group to be cyclic.

(b) Dihedral groups: Description, as a subgroup of S_n, matrix representation, generators and relations.

(c) $U_n := \mathbb{Z}_n^*$.

(d) Matrix groups such as $GL(n,\mathbb{R})$, $SL(n,\mathbb{R})$, $O(n,\mathbb{R})$, affine group and Euclidean motion group etc.

10 New Groups from the old

(1) Quotient groups; the importance of the first homomorphism theorem should be brought out in "identifying" the quotient group.

i. Examples of cosets; how to visualize it and look for a 'transversal' of representatives:

A. $H \leq G$, Define $\forall x,y\in G,\ \ x\sim y$ if $xH = yH$.

B. $G = \big(\mathbb{R}^2,+\big)$ and $H = \{y=0\}$

C. $G = \mathbb{C}^*$ and $H = S^1 = \{z\in\mathbb{C}/|z|=1\}$

D. $G = \mathbb{C}^*$ and $H = \mathbb{R}^+$.

E. $G = \mathbb{Z}$ and $H = m\mathbb{Z}$

F. $G = (\mathbb{R}^*,\cdot)$, $H = \{\pm 1\}$

G. $G = \mathbb{R}^*$ and $H := \mathbb{R}^+$.

H. $G = GL(n, \mathbb{R})$ and $H := SL(n, \mathbb{R})$.

I. $G = \mathbb{C}^*$ and H is the n-th roots of unity for a fixed $n \in \mathbb{N}$.

J. $G = S_n$ and $H := A_n$.

K. $ax + b$ group with H consisting of $(1, b)$.

ii. Examples of quotient groups. All the examples in the last item.

iii. Caution: $H \cong K \not\Rightarrow \frac{G}{H} \cong \frac{G}{K}$.

iv. $H_n \ncong H_m$ for $n \neq m$ but $\frac{G}{H_n} \cong \frac{G}{H_m}$.

v. Correspondence theorem.

Theorem 2. *Let G be a group and H a normal subgroup. Consider the quotient group G/H. Let $\mathcal{L}$ be the set of all subgroups of G/H and $\mathcal{K}$ be the subgroups of G containing H. Then the map*

$$\varphi \colon \mathcal{L} \to \mathcal{K}, \text{ given by } L \mapsto \pi^{-1}(L)$$

is a bijection.
Moreover, if L is a normal subgroup of G/K, then $K := \pi^{-1}(L)$ is a normal subgroup of G.
Finally, there is a bijection of $\pi^{-1}(L)$ with $L \times H$ for any $L \in \mathcal{L}$.

Proof. Let $L \in \mathcal{L}$ and let $K := \pi^{-1}(L)$. We show that K is a subgroup of G. Let $x, y \in K$. That is, $x, y \in \pi^{-1}(L)$. Hence $\pi(x), \pi(y) \in L$. Hence $\pi(xy) = \pi(x)\pi(y) \in L$, since L is a subgroup. This means that $xy \in \pi^{-1}(L) = K$. Similarly, if $x \in K$, $\pi(x) \in L$ so that $\pi(x)^{-1} \in L$. Since π is a group homomorphism, $\pi(x)^{-1} = \pi(x^{-1})$. Thus, $\pi(x^{-1}) \in L$ or $x^{-1} \in K$. Thus we have established that K is a subgroup of G. Also, if $x \in H$, $\pi(x) = eH$ and hence $\pi^{-1}(e) = H \subset K$. Thus $K \in \mathcal{K}$.
We now show that if L is normal in G/H, then $K := \pi^{-1}(L)$ is normal in G. Let $x \in K$ and $g \in G$. We have

$$\pi(gxg^{-1}) = \pi(g)\pi(x)\pi(g^{-1}) = \pi(g) \cdot \pi(x) \cdot \pi(g)^{-1}.$$

Since $\pi(x) \in L$ and L is normal in G/H, it follows that$\pi(g)\pi(x)\pi(g)^{-1} \in L$. We therefore conclude that $\pi(gxg^{-1}) \in L$. This means that $gxg^{-1} \in K$. Hence K is normal in G.
We now show that that map φ is a one-one. Let $L_1 \neq L_2 \in \mathcal{L}$. Hence there exists an element y in one of them and not in the other. Without loss of generality, assume that $y \in L_2 \setminus L_1$. Since π is onto, there exists $x \in G$ such that $\pi(x) = y$. We claim that $x \in K_2 \setminus K_1$. Since $\pi(x) = y \in L_2$, we see that $x \in K_2$. If $x \in K_1 = \pi^{-1}(L_1)$, it follows that $y = \pi(x) \in L_1$, a contradiction. Hence we conclude that $\varphi \colon \mathcal{L} \to \mathcal{K}$ is one-one.
We now claim that that φ is onto. Let $K \in \mathcal{K}$. Let $L := \pi(K)$. One easily shows that L is a subgroup of G/H. We claim that $K = \pi^{-1}(L)$ so that $\varphi(L) = K$. First of all, observe that $K \subset \pi^{-1}(L)$. For, if $x \in K$, then $\pi(x) \in \pi(K) = L$. Hence $x \in \pi^{-1}(L)$. We now show that $\pi^{-1}(L) \subset K$. Let $x \in \pi^{-1}(L)$. Thus, $\pi(x) = L$. But since $\pi(x) \in \pi(K)$, there exists $g \in K$ such that $\pi(x) = gH$. Recall that $\pi(x) = xH$, So we have $xH = gH$ or $g^{-1}x \in H$. Since $H \subset K$, we

see that $g^{-1}x \in K$. By choice $g \in K$ so that $x = g(g^{-1}x) \in K$. Thus $x \in K$. We have therefore shown that $\pi^{-1}(\pi(K)) = K$. This establishes that φ is onto. We have thus proved that $\varphi\colon \mathcal{L} \to \mathcal{K}$ is a bijection.
Let us now prove the last part. Let $L := \{g_iH : i \in I\}$. We claim that $\pi^{-1}(L) = \{g_ih : i \in I, h \in H\}$. For, let $x \in \pi^{-1}(L)$. Hence $\pi(x) \in L$. Thus we can find a $j \in I$ such that $\pi(x) = g_jH$. But by the very definition of π, we have $\pi(x) = xH$. It follows that $xH = g_jH$. We deduce that $g_j^{-1}x \in H$, say, $g_j^{-1}x = h$. Thus $x = g_jh$. Hence the claim is proved.
We now claim that all the elements in the set $\{g_ih : i \in I, h \in H\}$ are distinct. Let $g_ih = g_jh_1$. We get $g_j^{-1}g_i = h_1h^{-1} \in H$. It follows that $g_iH = g_jH$ and hence $g_i = g_j$. Since $g_ih = g_jh_1 = g_ih_1$, we find that $h = h_1$. Thus the claim is proved. The map $L \times H \to \pi^{-1}(L)$ given by $(g_iH, h) \mapsto g_ih$ is a bijection. □

vi. A special case of the last part: if G is finite, we have $|\pi^{-1}(L)| = |L||H|$.

vii. The result in the last part of the theorem is reminiscent of the following results from linear algebra.
Let $T\colon V \to W$ be an onto linear map. Fix $y \in W$. Since T is onto, there is $x \in V$ such that $Tx = y$. We claim that the set of all solutions of $Tx = y$ is the set $x + \ker T$. For, if $z \in \ker T$, then $T(x + z) = Tz + Tz = y + 0 = y$. Hence $x + \ker T \subset T^{-1}(y)$. Conversely, if $v \in V$ satisfies $Tv = y$, we than have $Tx - Tv = 0$ so that $T(x - v) = 0$. Thus, $x - v \in \ker T$, say $x - v = z \in \ker T$. We have $v = x - z \in x + \ker T$.

viii. Let us apply the last theorem.

Theorem 3. *Let G be a group of order p^n. Then for each r with $0 \le r \le n$ there exists a (normal) subgroup of order p^r.*

Proof. The proof is by induction on n. When $n = 1$, we have $|G| = p$ so that $r = 0$ or $r = 1$. The subgroups are accordingly the trivial and full groups.
Assume that the result holds true for groups of order p^{n-1} when $n \ge 2$.
Let G be a group of order p^n. Since G is a p-group, its center $Z(G)$ is not trivial so that $|Z(g)| = p^r$ with $r > 0$. By Cauchy's theorem, there exists an element $a \in Z(G)$ of order p. Since the cyclic group $< a > \subset Z(G)$, the subgroup $< a >$ is normal in G. (For, if $g \in G$, $ga^ig^{-1} = a^igg^{-1} = a_i$, since a_i commutes with all elements of G.)
The quotient group $G/ < a >$ is of order p^{n-1}. Let $0 \le r \le n - 1$. Then by indction hypothesis, there exists a subgroup $L \le G/ < a >$ whose order is p^r. By the last result, $K := \pi^{-1}(L)$ is a subgroup of G of order $|L|| < a > | = p^{r+1}$. Thus G has subgroups of order p^r, $1 \le r \le n$. The result is proved. □

ix. An abelian group is simple iff it is finite and of prime order.

(2) Exercises:

i. Let H be a nontrivial subgroup of S_n. Show that either $H \le A_n$ or exactly half of the elements in H are even permutations.
Hint: Look order at $H \to S_n \to S_n/A_n$.

ii. Let G be a nonabelian group. Assume that there exist homomorphisms from a group of order 12 and another of order 18 *onto* G. Identify G.

iii. Let N be a normal subgroup of a finite group G with index n. Let H be a subgroup of G with index m. Assume that $\gcd(m, n) = 1$. Show that $H \leq N$.

(3) Direct product of groups.

i. Let G, H be groups. Define a multiplication on $G \times H$ by $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$. Show that $G \times H$ is a group under this operation. $G \times H$ is called the *(external) direct product* of G and H.

ii. Prove that $G \times H$ and $H \times G$ are isomorphic.

iii. Show that $G \times H$ is abelian iff G and H are abelian.

iv. Find subgroups isomorphic to G and H in $G \times H$. Are they normal in $G \times H$? What is their intersection? Do elements of these subgroups commute with each other?

v. Generalize the last few item to a direct product of finite number of groups.

vi. Let $g = (g_1, \ldots, g_n) \in G_1 \times \cdots \times G_n$. Assume that each G_i is finite. Prove that

$$\operatorname{ord}(g) = \operatorname{lcm}(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_n)).$$

vii. Let G be a group. Let $H_i \leq G$, $1 \leq i \leq n$ satisfy the following conditions:
(i) Each H_i is normal in G.
(ii) $G = \langle H_i : 1 \leq i \leq n \rangle$.
(iii) For each i, we have $H_i \cap \langle H_j : 1 \leq j \leq n, j \neq i \rangle = \{e\}$.
Then G is isomorphic to the direct product $H_1 \times \cdots \times H_n$.

viii. Let G be a group and $H_i \leq G$, $1 \leq i \leq n$. Assume that each H_i is normal in G. If each $g \in G$ can be written uniquely as $g = h_1 h_2 \cdots h_n$ with $h_i \in H_i$, $1 \leq i \leq n$, then G is the direct product $H_1 \times \cdots \times H_n$.
This is similar to the (internal) direct sum definition of vector subspaces in linear algebra.

ix. Exercises:

(1) Prove or disprove $\mathbb{Z} \times \mathbb{Z}$ is cyclic.

(2) Let G, H be cyclic groups of order two. Show that $G \times H$ is isomorphic to Klein's 4–group.

(3) Show that any group of order 4 is either cyclic or isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(4) Find the number of elements of order 8 in $\mathbb{Z}_{16} \times \mathbb{Z}_{24}$.

(5) Let $\gcd(m, n) = 1$. Show that $U(mn)$ is isomorphic to $U(m) \times U(n)$.

(6) Express $GL(n, \mathbb{R})$ as a direct product of nontrivial groups.

(7) Consider $\Delta(G) := \{(x, x) : x \in G\}$. Show that $\Delta(G)$ is a subgroup of $G \times G$.

(8) When is $\{(x, x^{-1}) : x \in G\}$ a subgroup of $G \times G$?

(9) If p and q are distinct primes, find all subgroups of $\mathbb{Z}_p \times \mathbb{Z}_q$.

(10) Fix $m, n \in \mathbb{N}$. Can you identify $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : mx + ny = 0\}$ up to isomorphism?

(11) If $G \times H$ is cyclic, show that the groups G and H are finite cyclic groups.

(12) What is the largest order of any element in $\mathbb{Z}_{36} \times \mathbb{Z}_{42}$?

(13) Let G and H be cyclic groups of order 2 and 3 respectively. Find the orders of all elements of $G \times H$. Conclude that $G \times H$ is _____.

(14) Can you generalize part of the last exercise?

(15) Let H_1, H_2 be two *normal* subgroups of G such that $H_1 \cap H_2 = \{e\}$, $H_1H_2 = G$. Then G is isomorphic to the (external) direct product $H_1 \times H_2$. We say G is the *(internal) direct product* of H_1 and H_2.

(16) Let G be an (abelian) group of order 9. Show that G is either $\mathbb{Z}/(9)$ or $\mathbb{Z}/(3) \times \mathbb{Z}/(3)$.

(4) Semidirect product: Only if time permits.

11 Group actions

(1) Definition and a lot of geometric examples.

(2) Let X be a set, G a group. A *group action* of G on X is a map $\alpha : G \times X \to X$ given by
$\alpha(ab, x) = \alpha(a, \alpha(b, x))$ for all $a, b \in G$, $x \in X$.
$\alpha(e, x) = x$ for all $x \in X$.

We usually drop α and write $\alpha(g, x)$ as $g \cdot x$ or gx. Then (1) reads: $(ab) \cdot (x) = a \cdot (b \cdot x)$. We also say G *acts on* X and X is a G–set (when the action α is understood).

(3) Examples of group actions.

(a) $GL(n, \mathbb{R}) = \{n \times n$ invertible matrices $\}$ acts on $\mathbb{R}^n$.

(b) $O(n, \mathbb{R}) = \{n \times n$ orthogonal matrices $\}$ acts on $\mathbb{R}^n$.

(c) If X is any set, S_X, the symmetry group (of all bijections of X) acts on X.

(d) Let $G = \{\pm 1\}$. Let G act on $\mathbb{R}$ via $-1.x = -x$. Can you define an action of G on $\mathbb{R}^*$?

(e) Let $G = \{\pm 1\}$. We define two actions of G on $\mathbb{R}^2$.
(i) $-1 \cdot (x, y) := (y, x)$
(ii) $-1 \cdot (x, y) := (-x, -y)$.

(f) Any group G acts on itself via *left action:* $X = G$, $G \times X \to X$ given by $(g, x) \mapsto g \cdot x$, the group multiplication.

(g) A group G acts on itself via *conjugation:* $(g, x) \mapsto gxg^{-1}$. The orbits are called *conjugacy classes.*

(4) The *orbit* of G in X is a set of the form $G \cdot x = \{g \cdot x \mid g \in G\}$ for a fixed $x \in X$. $G \cdot x$ is also called the *orbit of* x, denoted by $\mathcal{O}_x$. Note that $y \in Gx$ iff $y = gx$ for some $g \in G$ iff $x = g^{-1}y$ for some $g \in G$ iff $x \in Gy$. Thus $Gx = Gy$ iff $\mathcal{O}_x = \mathcal{O}_y$. Define an equivalence relation $x \sim y$ iff $Gx = Gy$. Its equivalence classes are orbits of G in X and X is the disjoint union of orbits of G.

(5) Exercises:

(a) Find the orbits in the above examples. Draw pictures of orbits whenever possible.

(b) What are the orbits in Example 3g if G is abelian?

(c) Let $H \leq G$. Let H act on $X = G$ via the left action: $(h, x) \mapsto hx$. The orbits are of the form Hx for some $x \in G$. Note that $Hx = Hy$ iff $xy^{-1} \in H$. Write $G = \cup_{x \in G} Hx$. Any two orbits are bijective via the map $h \to hx$. If G is finite we deduce Lagrange's theorem.

(6) G acts *transitively* on X if for any $x, y \in X$, there is a $g \in G$ such that $gx = y$. That is, there is only one orbit in X.

Which of the actions in Example 3a to Example 5c are transitive?

(7) Fix $x \in X$. Let $G_x := \{g \in G \mid gx = x\}$. Then G_x is called the *stabilizer* of x in G and is a subgroup. G_x is also called the *isotropy* subgroup of x.

(a) Let $\mathcal{O}_x = \mathcal{O}_y$. How are the stabilizers G_x and G_y related?

(b) Find the stabilizers of various elements in the above six examples.

(c) Every subgroup H of a group G occurs as a stabilizer of an element in a G–set. *Hint:* Let $X = \{Hg \mid g \in G\}$ be the set of (right) cosets, i.e., the orbits of H in G with respect to the left action of H on G. Then $|X| = [G : H]$, the index of H in G. G acts on X by $(a, Hg) \mapsto Hga^{-1}$. (If Y is the set of left cosets, i.e., $X = \{gH \mid g \in G\}$, then G on Y by $(a, gH) \mapsto agH$). This action is transitive. If $x = H \in X$, then the stabilizer of x is H.

(8) Let X and Y be two G–sets. Then these are G–*isomorphic* if there is a bijection $f : X \to Y$ such that $g \cdot f(x) = f(g \cdot x)$ for all $g \in G$, $x \in X$. Draw a commutative diagram.

(9) Let G act transitively on X. Then X is G–isomorphic to G/H (the set of left cosets of H in G) for some subgroup $H \leq G$. *Hint:* H is the stabilizer of a fixed $x \in X$.

(10) $|\mathcal{O}_G(x)| = |G \cdot x| = [G : G_x]$. ($G$ acts on X, $x \in X$).

(11) Let G act on itself via conjugation. Then $G_x = \{g \in G \mid gx = xg\}$ is known as the *centraliser* $Z_x(G)$ of $x \in G$. $G \cdot x = C_x$ is called the *conjugacy class* of x in G. Note that $|C_x|$ is a divisor of $|G|$ if G is finite. If G is finite and $\{C_1, \ldots, C_r\}$ are disjoint conjugacy classes, then $|G| = |C_1| + \cdots + |C_r|$ is called the *class equation*. Note that $G = |Z_G| + \sum_{i=1}^{r} [G : G_{x_i}]$ if $\{G \cdot x_i\}$ are the distinct conjugacy classes of G with $|G \cdot x_i| > 1$.

(12) Exercises:

(1) Use the class equation to prove that if $|G| = p^r$, then $Z(G)$, the center of G is non-trivial.

(2) Let $[G : Z(G)] = n$. Show that any element has at most n conjugates.

(3) Let G act on X and Y. Define a G action on $X \times Y$ in an obvious way. Relate the stabilizer of (x, y) with those of x and y.

(4) Let G be a group and let H, K be subgroups of index r and s respectively. Show that $H \cap K$ has index at most rs.

(5) Let G be a group, H, K subgroups of G of index r. Assume H and K are conjugate. Show that $H \cap K$ has index at most $r(r-1)$.

(6) Let $\{c_i\}$ be the conjugacy classes in a group. Show that each product $C_i C_j$ is a union of conjugacy classes.

(7) Determine all subgroups with only two conjugacy classes.

(8) Let $H \leq G$. Let $X = \{xH \mid x \in G\}$. Let G act on X by $(g, xH) \mapsto gxH$. Prove that H is a normal subgroup of G iff every H–orbit in X is a singleton.

(9) Let $|G| < \infty$ and let p be the smallest prime dividing $|G|$. Let $H \leq G$ such that $[G : H] = p$. Show that H is a normal subgroup of G.

(10) Recall the class equation: G acts on itself via conjugation. Therefore $|G| = |\mathcal{O}_1| + \cdots |\mathcal{O}_r|$, $|O_i| = \{gxg^{-1} \mid g \in G\} = \mathcal{O}_x$. $|G| := |Z(G)| + \sum_{i=1}^{r} |[G : C_G(x)]|$ in classical notation.

(11) Let p be a prime and $|G| = p^n$. Then G has a non-trivial centre. *Hint:* Apply class equation. Note that $x \in Z(G)$ iff $|\mathcal{O}_x| = 1$.

(12) Let G be a p-group. If H is a proper subgroup of G, show that $H \subsetneq N_G(H)$.
Hint: Choose $z \in Z(G)$. If $z \in H$, consider the quotient group $G/\langle z \rangle$ and use induction.

(13) If p is a prime and $|G| = p^2$, then $G \simeq \mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$.

(14) Let $H \leq G$ with $[G : H] = n$. Show that H contains a normal subgroup K of G such that $[G : K] \leq n!$.

(15) Let G be a simple group (i.e., having no proper normal subgroup) with a subgroup H of finite index $n > 1$. Show that $|G| \leq n!$.

(16) Let G be a p-group and N a normal subgroup of G. Show that $N \cap Z(G) \neq \{e\}$.
Hint: Let G act on $N \setminus \{e\}$ by conjugation. Does it have a fixed point?

(17) Let G be a group with a conjugacy class containing exactly two elements. Show that G has a proper normal subgroup.

(18) Let G be nonabelian group of order p^3 where p is a prime. Show that
(i) $|Z(G)| = p$.
(ii) $Z(G)$ is the commutator subgroup of G.

(13) Applications of Group action

(a) Groups of even order have an odd number of elements of order 2.

(b) Lagrange's theorem.

(c) Cauchy's theorem

Theorem 4 (Cauchy's Theorem)**.** *. Let G be a finite group and p a prime such that $p \mid |G| = n$. Then there exists an element of order p in G.*

Proof. Let $X = \{(x_1, \ldots, x_p) \mid x_1 \cdots x_p = 1\}$, $|X| = n^{p-1}$. Let σ be the n–cycle $(12 \cdots p)$. Then σ acts on X. $(x_1 \cdots x_p) \sim (y_1 \cdots y_p)$ if $\sigma^r(x_1 \cdots x_p) = (y_1 \cdots y_p)$. The orbits of σ or equivalence classes have either one element or p elements. If m is the number of orbits with one element, then $n^{p-1} = kp + m$. Hence $p \mid m$. □

(d) A Fixed Point theorem.

Theorem 5. *Let G be a p-group. Assume that G acts on a finite set X. Let $X_0 \equiv X^G$ denote the set of fixed points of the action by G. That is, $X_0 := \{x \in G : gx = x \text{ for all } g \in G\}$. We have*

$$|X_0| \equiv |X| (\,(\mathrm{mod}\, p)). \tag{3}$$

Observe that in the orbit decomposition of X, any non-singleton orbit will be a positive power of p.

(e) Let G be a finite group. Assume that for any two subgroups H and K of G, we have either $H \leq K$ or $K \leq H$. Prove that G is of prime power order.

Hint: There cannot be two distinct prime divisors of $|G|$. If $a \in G$ is of maximal order, then for any $x \in G$, what is the relation between $\langle x \rangle$ and $\langle a \rangle$?

(f) Any group of order 6 is isomorphic to $\mathbb{Z}/(6)$ or to the dihedral group D_3.

By Cauchy's theorem, there exists $x, y \in G$ such that $\mathrm{ord}(()x) = 3$, $\mathrm{ord}(y) = 2$. Cosets $\langle x \rangle \cup \langle x \rangle\, y = \{e, x, x^2, y, xy, x^2y\} = G$. This implies $yx \in \{e, x, x^2, y, xy, x^2y\}$, $yx \notin \langle x \rangle$. Also, $yx \neq y$. Hence $yx = xy$ or $yx = x^2y$. The former implies $G \simeq \mathbb{Z}_6$ and the latter implies $G \simeq D_3$. □

(g) The *quaternion group* has generators i, j, k with relations $i^2 = j^2 = k^2 = -1$, $ij = -jk = k$. It has eight elements and is non-abelian and denoted by $\mathbf{Q}$.

(h) A matrix representation of $\mathbf{Q}$: Let $A := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. We have

$$\mathbf{Q} = \{I, A, A^2, A^3, B, BA, BA^2, BA^3\}.$$

Prove that $\mathbf{Q}$ is a nonabelian group of order 8 Each non-identity element g satisfies $g^2 = -I$. The only element of oder 2 is $-I$ and it lies in the centre of $\mathbf{Q}$.

(i) Show that the $\mathbf{Q}$ and D_8 are not isomorphic.

(j) A group of order eight is isomorphic to one of the five: $\mathbb{Z}/(8)$, $\mathbb{Z}/(4) \times \mathbb{Z}/(2)$, $\mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2)$, D_4, Q.

Let G be a group with $|G| = 8$. If G is cyclic, then $G \simeq \mathbb{Z}/(8)$. Suppose that the largest order of an element is four. Choose $x \in G$ with $\mathrm{ord}(()x) = 4$. Take $y \notin \langle x \rangle$. Then $\langle x \rangle \cup \langle x \rangle\, y = G = \{e, x, x^2, x^3, y, xy, x^2y, x^3y\}$. This implies $yx \notin \langle x \rangle$ and hence $yx \neq y$. If $yx = x^2y$, then $yxy^{-1} = x^2$ and hence $4 = \mathrm{ord}(()x) = \mathrm{ord}(x^2) = 2$. Therefore $yx \neq x^2y$. Therefore $yx = xy$ or $yx = x^3y$. Now $y^2 \notin \langle x \rangle\, y$ (otherwise $y \in \langle x \rangle$). Also, $y^2 \neq x, x^3$ (otherwise $\mathrm{ord}(y) = 8$). Hence if y has order 4, then $y^2 = x^2$.

Case 1. $yx = xy$ and $y^2 = e$. The map $x \mapsto (1, 0)$, $y \mapsto (0, 1)$ in $\mathbb{Z}/(4) \times \mathbb{Z}/(2)$ implies that $G \simeq \mathbb{Z}/(4) \times \mathbb{Z}/(2)$.

Case 2. $yx = x^3y$ and $y^2 = e$. The map $x \mapsto r$, $y \mapsto s$ yields $G \simeq D_4$.

Case 3. $yx = xy$ and $y^2 = x^2$. G is abelian and $\mathrm{ord}(xy^{-1}) = 2$ (since $(xy^{-1})^2 = x^2y^{-2} = e$). The maps $x \mapsto (1, 0)$, $xy^{-1} \mapsto (0, 1)$ implies that $G \simeq \mathbb{Z}/(4) \times \mathbb{Z}/(2)$.

Case 4. $yx = x^3y$ and $y^2 = x^2$. The maps $x \mapsto i$, $y \mapsto j$ implies $G \simeq Q$.

Case 5. $\mathrm{ord}(()x) = 2$ for all $x \neq e$. G is abelian. Choose $x, y, z \in G$, $x, y, z \neq e$ $x \neq y$, $z \neq xy$. $H = \{e, x, y, xy\} \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2)$, $K = \{e, z\}$. Then $HK = G$ and $H \cap K = \{e\}$. Hence $G \simeq H \times K = \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. □

(k) Let H be a subgroup of S_n and $H \subseteq A_n$. Prove that precisely one half of the elements of H are even permutations. *Hint:* You do not need Cauchy's theorem!

(l) Let G be a group of order $4n + 2$. Use Cayley's theorem, Cauchy's theorem and the last exercise to prove that G contains a group of order $2n + 1$.

(m) Let $p_1, \ldots, p_n$ be distinct primes. Show that an abelian group of order $p_1 \cdots p_n$ must be cyclic.

(n) Prove that a group of order 10 is either isomorphic to $\mathbb{Z}/(10)$ or D_5.

(o) Let p be an odd prime. Then any group of order $2p$ is cyclic or dihedral.
$\mathrm{ord}(x) = p$, $\mathrm{ord}(y) = 2$. Then $\langle x\rangle \cup \langle x\rangle\, y = G$, $\langle x\rangle \leq G$. $\mathrm{ord}(xy) = 2, p$ or $2p$. $xyxy = e$ implies $yx = x^{-1}y$. Hence $G = D_p$. $\mathrm{ord}(xy) = 2p$ implies G is cyclic. $\mathrm{ord}(xy) = p$ cannot arise. For, $\langle x\rangle = \langle x\rangle\,(xy)^p = (\langle x\rangle\, xy)^p = (\langle x\rangle\, y)^p = \langle x\rangle\, y^p = \langle x\rangle\, y$. □

(p) Class equation: application to p-groups.

(q) Cayley's theorem and its generalizations

(r) A subgroup of index p, the smallest prime divisor of $|G|$.

12 Sylow's Theorems

Sylow's theorems: It is advisable to give the standard induction proof as well as the group action proof for the first Sylow. The other two are proved by group actions. Typical examples should also introduce the students to some counting arguments.

1. An observation. Let $S \subset G$ be such that the left translates $\{gS : g \in G\}$ are either the same or pairwise disjoint and their union is G. Then there exists a subgroup H such that S is a left coset of H and hence all the translates of S are cosets of H.

   Since the union of the translates of S is G, there exists $a \in G$ such that $e \in aS$. We claim that $H := aS$ is a subgroup. If $x \in H$, then $x^{-1}H = x^1 aS$ contains e $e \in H$. Since the only translate of S which contains e is H, it follows that $x^{-1}H = H$. Since $e \in H$, $x^{-1}e \in x^{-1}H = H$. We have thus shown that if $x \in H$, so is x^{-1}. Let $x, y \in H$. Then $e \in xH$ and hence $xH = S$. But $y \in H$ and so $xy \in xH = H$. Thus H is a subgroup.

2. **Sylow-1:** Let p be a prime. Let $|G| = p^r m$. (p may still divide m.) Let n_r be the number of subgroups of order p^r. Then $n_r \equiv 1(\,(\mathrm{mod}\, p))$. In particular, G does have a subgroup of order p^r.

   Let X be the set of subsets of order p^r in G. We let G act on X via $(g, S) \mapsto gS$. Let G_S denote the stabilizer subgroup of $S \in X$. We make three observations:
   (i) Since $G_S \cdot S = S$, it follows that S is a union of cosets of G_S and hence $|G_S| = p^s$ for some $s \leq r$.
   (ii) For any $S \in X$, the union of the elements in the orbit of S is G. For, if $g \in G$ and $s \in S$, then $x \in xs^{-1}S \in G \cdot S$.
   (iii) The orbit $G \cdot S$ contains $|G|/|G_S|$ elements.

   The orbits in X are of two kinds:

   (i) First kind: No intersection among the elements of the orbit. In view of the observation in the last item, it follows that the element (of the orbit) containing e will be a subgroup of order p^r and the orbits is the set of cosets of this subgroup.

   (ii) There are intersection between elements of the orbit. In this, there will be more number of elements in the orbit as their union has to cover all of G. As a consequence, $|G \cdot S| = |G|/|G_S| = p^t m$ with $t \geq 1$.

Let n_r be the number of orbits of first kind and k that of the second kind. Hence

$$|X| \equiv n_r \times m(\,(\mathrm{mod}\, p)m).$$

We shall find a different congruence relation for $\binom{p^r m}{p^r}$. Let C be the cyclic group of order $p^r m$. It has a unique subgroup of order p^r. Hence $n_r = 1$ in this case. Hence we arrive at the following:

$$\binom{p^r m}{p^r} \equiv m(\,(\mathrm{mod}\, p)m).$$

Thus we have $\binom{p^r m}{p^r} \equiv n_r m \equiv m(\,(\mathrm{mod}\, p)m)$. Therefore, $m(n_r - 1) \equiv 0(\,(\mathrm{mod}\, p)m)$ and so $n_r \equiv 1(\,(\mathrm{mod}\, p))$.

2nd Proof by Induction. We shall prove that for any divisor p^r of $|G|$, there exists a subgroup of that order.

If $|G| = 1$, the result is true. Assume that the result is true for all groups of order less than n. Let G be a group of order n and $p^r \mid |G|$.

Case 1: p divides $|Z(G)|$. By Cauchy's theorem (easy for abelian groups), there exists an element $a \in Z(G)$ of order p. The subgroup $\langle a \rangle$ is normal in G (why?). Hence we can form the quotient group $G/\langle a \rangle$. Its order is less than n and it is divisible by p^{r-1}. By induction there exists a subgroup $\overline{H} \leq G/\langle a \rangle$ whose order is p^{r-1}. The pull-back $H := \pi^{-1}(\overline{H})$ is a subgroup of order p^r.

Case 2: p does not divide $|Z(G)|$. We now exploit the class equation.

$$n = |G| = |Z(G)| + \sum_a [G : N_G(a)],$$

where the sum is taken over representatives of equivalence class with more than one element. Now, $p \mid n$ and p does not divide $|Z(G)|$. We conclude that there exist at least one $a \in G \setminus Z(G)$ such that p does not divide $[G : N_G(a)]$. Consequently, $p^r \mid |N_G(a)|$. Since $|N_G(a)| < n$, by induction there exists a subgroup $H \leq N_G(a)$ whose order is p^r. Of course, H is a subgroup of G with order p^r. □

3. **Sylow-2:** Let $H \leq G$ be a subgroup and P a Sylow p-subgroup of G. Then there exists $x \in G$ such that $xHx^{-1} \subset P$. In particular, any two Sylow p-subgroups are conjugate.

   Let S be the set of left cosets of P. Let H act on S by left action. We have

   $$S_0 \equiv S^H \equiv |S| = [G : P](\,(\mathrm{mod}\, p)).$$

   Since p does not divide $[G : P] = m$, p does not divide S_0. In particular, $|S_0| \neq 0$. Hence $|S_0| \geq 1$.

   Thus, there exists $x \in G$ such that $hxP = xP$ for any $h \in H$. But this means $x^{-1}hx \in P$ for all $h \in H$. That is, $xHx^{-1} \leq P$. □

4. **Sylow-3:** The number of Sylow p-subgroups divides $|G|$ and it is of the form $1 + kp$ for some $k \geq 0$.

   This is already part of Sylow-1. We give another proof. Fix a Sylow p-subgroup P. Let S be the set of all Sylow p-subgroups. Let P act on S by conjugation. Recall that

S is the set of conjugates of P by Sylow-2. Hence $|S| = [G : N_G(P)]$, is a divisor of $|G|$. Now $H \in S_0$ iff $xHx^{-1} = H$ for all $x \in P$. This happens iff $x \in N_G(H)$ for all $x \in P$. Therefore, we conclude that if $H \in S_0$, we have $P \leq N_G(H)$. But then P and H are both Sylow p-subgroups of $N_G(H)$. Since H is normal in $N_G(H)$ and all Sylow p-subgroups in $N_G(H)$ are conjugate, it follows that $H = P$. Thus $|S_0| = 1$. From the fixed point theorem, we deduce

$$|S| \equiv |S_0| \equiv 1(\,(\mathrm{mod}\, p)).$$

5. Observe that we have three conditions on N_p:
   - $N_p \equiv 1(\,(\mathrm{mod}\, p))$.
   - $N_p = [G : N_G(p)]$ is a divisor of $|G|$.
   - Since $P \leq N_G(P)$, we see that N_p is a divisor of $[G : P]$.

6. Examples.

   (1) Groups of order 15: By Sylow-1, there exists a subgroup H of order 5. The number of such 5-subgroups are of the form $1 + k5$ and it divides 15. Thus among 1, 6, 11 the only number which divided 15 is 1. Hence H is normal in G and hence G is not simple.

   We can say more. Let K be a 3-subgroup of G. The number of such subgroups is of form $1 + 3k$ and is a divisor of 15. Thus the only possibility is 1. Thus K is normal in G. Also $H \cap K = \{e\}$. (Why?)

   From these information, we can conclude that G is a cyclic group of order 15. For, let $H = \langle a \rangle$ and $K = \langle b \rangle$. Observe that

   $$H \ni a(ba^{-1}b^{-1}) = aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in K.$$

   Hence we see that $aba^{-1}b^{-1} = e$ or $ab = ba$. Since the orders of these two commuting elements are co-prime, the order of ab is 15. Thus the sybgroup generated by ab is all of G.

   (2) $|G| = 56$. The possibilities of n_7 are 1, 8 and 15. If $n_7 = 1$, then the Sylow 7-subgroup is normal and hence G is not simple.

   If $n_7 = 8$, then these eight Sylow 7-subgroups account for $8 \times 6 = 48$ elements. This leaves us with 8 elements which should constitute the Sylow 2-subgroup. Hence the Sylow 2-subgroup is normal. We therefore conclude that any group of order 56 is not simple.

   (3) Groups of order 36: That these are not simple can be seen as above. We illustrate another powerful method in the employment of group actions. Let H be a Sylow 3-subgroup. Its index is 4. Let G act on the cosets G/H via left action. Thus we have a homomorphism $\varphi\colon G \to S_4$.

   $\ker\varphi \neq (e)$: For, then φ is one-one and hence $36 = |G| = |\varphi(G)| \leq |S_4| = 24$, a contradiction.

   $\ker\varphi \neq G$: For, $g \in \ker\varphi$ iff $gxH = xH$ for all $x \in G$, that is same as saying that $x^{-1}gx \in H$ or $g \in xHx^{-1}$. Thus, $\ker\varphi = \cap_{x\in G} xHx^{-1} \subset H \subsetneq G$.

   Since G has a nontrivial proper normal subgroup, G is not simple.

(4) Group of order 48:

We claim that it has a normal subgroup of order 16 or 8. If there is only one Sylow subgroup, then it is a normal subgroup of order 16. So assume that there exist two Sylow subgroups of order 16, say, H and K. Now $L := H \cap K$ is a subgroup. To compute its order we use the product formula:

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

If $|H \cap K| \leq 4$, then $|HK| \geq (16 \times 16)/4 = 64$, an absurdity. Hence $|H \cap K| = 8$. Since the index of $H \cap K$ in H (or in K) is 2, it is normal in H and K. Hence the normalizer N of $H \cap K$ must contain both H and K. Since $H, K \leq N$, 16 must divide $|N|$ and $|N|$ must therefore be $m \times 16$ where $m > 1$. Also, $|N|$ is a divisor of 48. It follows that $|N| = 48$ or $N = G$. Thus $H \cap K$ is normal in $G = N$.

(5) Any group of order 108 has a normal subgroup of order 27 or 9. (Similar to the last item.) Only point to worry is: Why is $H \cap K$ normal in H and K? You may observe that any subgroup of order p^{n-1} in a group of oder p^n is normal.

(6) No group of order 36 is simple. Similar to the last two examples.

(7) No group of order 30 is simple. Assume otherwise and count the number of elements in all (5) Sylow 5-subgroups and all (10) Sylow 3-subgroups. Conclude that either there is only Sylow 5-subgroup or Sylow 3-subgroup.

(8) Groups of order pq: Let p and q be primes with $q > p$.

- The Sylow q-subgroup is normal and hence G is not simple.
  The number of N_q of Sylow q-subgroups is of the form $1 + kq$ and it must divide pq and hence p. Therefore, $N_q = 1$.
- If p does not divide $q - 1$, then G is cyclic.
  Since $N_p = 1 + kp$ divides q, it follows p divides $q - 1$ if $k \geq$. Hence $N_p = 1$. Thus $P = \langle x \rangle$ and $Q = \langle y \rangle$ are cyclic, normal and $P \cap Q = \{e\}$. Elements of P and Q commute: $Q \ni (xyx^{-1})y^{-1} = xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in P$. Hence $\mathrm{ord}(xy) = pq$.

(9) Groups of order p^2q:

If $p > q$, by the argument standard by now, we see that P is normal in G.

If $p < q$, and if Q is not normal, count the number of non-identity elements in all Sylow q-subgroups. Conclude that there are $p^2(q-1)$ elements of oder q. The remaining $p^2q - p^2(q-1) = p^2$ elements must be in P, the unique Sylow p-subgroup. Work out the details.

(10) The number of Sylow subgroups in A_5.

Note that any element of A_5 is one of the following cycle types: (221), (311), (5).

If $p = 2$, then $n_2 \equiv 1 (\mathrm{mod}\, 2)$ is a divisor of $[G : P] = 60/4 = 15$. Hence we find that N_2 is either 1, 3, 5 or 15. There are $5 \times 3 = 15$ elements of order 2. In each Sylow 2-subgroup there will be 3 non-identity elements and hence e they fill up at least 5 Sylow 2-subgroups. Hence $N_2 \geq 5$. Can it be 15? If $N_2 = 15$, then $N_G(P) = P$. For $P \leq N_G(P) \leq G$ and $15 = N_2 = [G : N_G(P)] \leq [G : P] = 15$. So, this says the only elements of A_5 normalizing P are in P. But then a 3-cycle normalizes P.

Details!

(11) Groups of order p^2.

(12) Let G be nonabelian and $|G| = p^r m$ with p a prime. Assume that , $m > 1$ and p^r does NOT divide $(m-1)!$. Then G is not simple.

Assume that such a group is simple. Let P be the Sylow on p-subgroup of index m. Letting G act on the left cosets of P, we get a homomorphism $\varphi\colon G \to S_m$ with $\ker\varphi \leq P$. Simplicity of G implies that $\ker\varphi = \{e\}$. But then $G \cong \varphi(G) \leq S_m$. Hence we conclude that $p^r m$ divides $m!$ and hence p divides $(m-1)!$.

(13) All groups up to order 60 are simple.

If p is a prime, then every p-group has a non-trivial center. If G is abelian, any of its proper subgroup (which exist) is normal and hence G is not simple. If G is nonabelian, $Z(G)$ is a proper nontrivial normal subgroup and hence is not simple.

Now, the only integers n between 2 and 59, neither a prime power nor having a factorization of the form $n = p^r m$ as in the last item are $n = 30, 40,$ and 56. By the last item, these three numbers are the only candidates for orders of nonabelian simple groups of order less than 60.

We have already seen groups of order 30 and 56 are not simple. We claim that no group of order 40 is simple.

Let G be a group of order 40, and let P be a Sylow 5-subgroup of G. We have N_5 divides $40/5 = 8$ and and $N_5 \equiv 1(\,(\mathrm{mod}\,5))$. These conditions force $N_5 = 1$, so that P is normal in G. Therefore, no simple group of order 40 can exist.

(14) Groups of order 6

(15) Groups of order 8

(16) Simplicity of A_5.

- $|A_5| = 60 = 2^2 \times 3 \times 5$.
- There are 24 elements of order 5 in A_5: $\frac{5\times4\times3\times2}{5}$.
- There are 20 elements of order 3 in A_5: $\frac{5\times4\times3}{3}$.
- Elements of order 2 in A_5 are of the form $(ab)(cd)$, product of two disjoint transpositions. There are 15 elements of order 2 in A_5: $\frac{1}{2} \times \left(\frac{5\times4}{2} \times \frac{3\times2}{2}\right)$.
- Let N be a proper normal subgroup of A_5. We claim that N is trivial.
- Let 5 divide $|N|$. Since N is normal, all 24 elements of order 5 are in N. Hence $|N| \geq 24$. Since $|N|$ also divides $|A_n| = 60$, we see that $|N| \geq 30$.
- Let 3 divide $|N|$. Again the normality of N forces us to conclude that all 20 cycles of length 3 lie in N. Hence $|N| \geq 20$.
- Since we assume that N is proper, if either 3 or 5 divide $|N|$, we conclude that $|N| = 30$. Since both 3 and 5 divide $|N|$, we have $|N| \geq 20 + 24 = 44$ by the last two observations, a contradiction.
- We are thus lead to the conclusion that $|N|$ must be a power of 2.
- Let $|N| = 4$. Since N is normal, it follows that N must the unique Sylow 2-subgroup of A_5. Hence all elements of order 2 must lie in N. But there are 15 of them! Hence $|N| \neq 4$.
- We are thus left with the only possibility $|N| = 2$. Then A_5/N is a group of order 30. Either its Sylow 5-subgroup or its Sylow 3-subgroup is normal. (For, if it were false, then G/N will have 6 Sylow 5-subgroups and 10 Sylow 3-subgroups. So, G/N must have $(6\times4)+(10\times2) = 44$ elements.) If K is a proper

normal subgroup of G/N, then its pull-back by the quotient map $A_5 \to A_5/N$ will be a normal subgroup of order either 2×5 or 2×3. In particular, N would be a proper normal subgroup whose order is either divisible by 5 or by 3. But we have seen no such normal subgroup exists in A_5. Thus $|N| = 2$ is also ruled out. Thus any proper normal subgroup of N is the trivial subgroup. In other words, A_5 is simple.

(17) Another proof of simplicity of A_5.

- Let N be a normal subgroup of a finite group. Assume that $x \in G$ is such that $\gcd(\text{ord}(x), |G/N|) = 1$.
  Look at xN. We have $\text{ord}(xN) \mid \text{ord}(x)$ and $\text{ord}(xN) \mid |G/N|$. Hence $\text{ord}(xN) = 1$. Hence $xN = N$ and so, $x \in N$.
- Let N be normal in A_5. Assume $|N| > 1$. The possible orders of N are 2,3,4,5,6,10,12,15,20 or 30.
- Let $|N| = 5, 10, 15$ or 20. Then $\gcd(5, |G/N|) = 1$. Hence any element of order 5 lies in N. Hence $|N| > 24$, a contradiction. So, no such normal subgroup exists in A_5.
- Let $|N| = 3, 6$ or 12. Again, $\gcd(|N|, |G/N|) = 1$. Hence N contains all elements of order 3. Thus $|N| \geq 20$. So, no such normal subgroup exists in A_5.
- Let $|N| = 4$ or 12. We have $\gcd(2, |G/N|) = 1$. Hence all 15 elements of order 2 lie in N. So, no such normal subgroup exists in A_5.
- Let $|N| = 30$. Then $|G/N| = 2$. Hence 24 elements of order 5 and 20 elements of order 3 lie in N. Thus $|N| \geq 44$. We conclude no normal subgroup of order 30 exists in A_5.
- Let $|N| = 2$. Then A_5/N is a group of order 30. Either its Sylow 5-subgroup or its Sylow 3-subgroup is normal. For, if it were false, then G/N will have 6 Sylow 5-subgroups and 10 Sylow 3-subgroups. So, G/N must have $(6 \times 4) + (10 \times 2) = 44$ elements. If K is a proper normal subgroup of G/N, then its pull-back by the quotient map $A_5 \to A_5/N$ will be a normal subgroup of order either 2×5 or 2×3. But we have seen no such normal subgroup exists in A_5.

(18) **Exercises:**

(1) Let two distinct primes p and q divide $|G|$. Assume that G has a unique Sylow p-subgroup of G. Show that G is not simple.

(2) Let $|G| = 63$. Show that Sylow 7-subgroup is normal and hence G is not simple.

(3) Let p be a prime. Find the number Sylow p-subgroup of S_p.
Ans: $(p-2)!$. *Hint:* For, they are generated p-cycles. There are $(p-1)! = p!/p$ of such cycles. But each cycle gives rise to a Sylow p-subgroup and the number of generators of each is $p - 1$.

(4) Show that any group of order $p^r m$ with $m < p$ is not simple.

(5) Let G be a noncyclic group of order 21. Show that G has 14 elements of order 3.

(6) Let $|G| = 48$. Show that any two distinct Sylow 2-subgroups must have 8 elements common.

(7) Let G be a finite group. Assume that the order every element is a power of a fixed prime p. Show that G is a p-group.

(8) Let H be a normal p-subgroup. Show that H is a subgroup of any Sylow p-subgroup.

(9) Let H be a normal subgroup of G. Assume that $[G : H]$ is coprime to p. Then H contains each of the Sylow p-subgroup.

(10) G is a direct product of its Sylow groups iff each of its Sylow subgroups is normal.
Let $n = |G| = p_1^{n_1} \cdots p_k^{n_k}$ be the prime decomposition. Let $P - i$ be the unique Sylow p_i-subgroup. Consider the map

$$f \colon P_1 \times \cdots \times P_k \to G \text{ defined by } f(x_1, \ldots, x_k) = x_1 \cdots x_k.$$

We claim that f is an isomorphism. By standard argument, $x_i x_j = x_j x_i$ where $x_r \in P_r$. Hence it follows that f is a group homomorphism. Let $f(x_1, \ldots, x_k) = x_1 \cdots x_k = e$. For any i, we have $x_i^{-1} = x_1 \ldots x_{i-1} x_{i+1} \cdots x_k$. Since p_i divides $\text{ord}(x_i)$ and $x_i \in P_1 \cdots P_{i-1} P_{i+1} \cdots P_k$, we see that $\text{ord}(x_i)$ is a divisor of $p_1^{n_1} \ldots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}$, it follows thatord$(x_i) = 1$. Thus $x_i = e$ for all i. Thus f is one-one. Since $|G| = |P_1 \times \cdots \times P_k|$, f is onto.

(11) Use Sylow's theorem to prove that A_4 does not have a group of order 6.
Let $H \leq A_4$ be of order 6. If P is Sylow 3 -subgroup of H, then P is of index 2 and hence normal in H. There are 8 Sylow-subgroups in A_4 and all of them are normal in A_4. They all lie in H now.

(12) Show that any subgroup of order 11 in a group of order 99 is normal.

(13) Let H be a p-subgroup of a finite group G. Show that H is a Sylow p-subgroup iff p does not divide $[G : H]$.

(14) Let N be a normal subgroup of G. Assume that P is a Sylow p-subgroup of G and that $P \subset N$. Show that the number of Sylow p-subgroup of N is the same as that of G.

(15) Let P be a normal Sylow p-subgroup of a finite group G. Let $f \colon G \to G$ be a homomorphism. Prove that $f(P) \leq P$.

(16) Let N be a normal subgroup with $|N| = p^n$ in a finite group G. Show that $N \leq P$ where P is any Sylow p-subgroup of G.

(17) Let G be a nonabelian with $|G| = pq$, product of distinct primes. Prove that $Z(G) = \{e\}$.

(18) Let $|G| = 2m$ with m odd. Show that there exists exactly one element of order 2.
Hint: Let $\text{ord}(x) = 2$. The number of Sylow subgroups is odd and it is $|C_G(x)|$. Hence $|C_G(x)|$ is even and let $y \in C_G(x)$ be of order 2. What can you do with $\langle x, y \rangle$?

(19) Let $|G| = p^m q^n$ where p and q are distinct primes. Assume that p does not divide $q^k - 1$ for $1 \leq k \leq n$. Prove that G has a unique Sylow p-subgroup and hence G is not simple.
List numbers of this form and are at most 100.

(20) Let G be of finite order n. Assume that for each divisor d of n, there exist at most d elements of order d. Prove that G is cyclic.
Hint: Let P be Sylow p-subgroup order p^m. Since $1 + p + \cdots + p^{m-1} < p^m$, conclude that P is cyclic. Show that P is the only Sylow p-subgroup. Hence it is normal. It follows that G is direct product of its Sylow p-subgroups.

(21) Let G be finite. Let $f\colon G \to H$ be an onto homomorphism.
(i) If P is Sylow p-subgroup of G, show that $f(P)$ is a Sylow p-subgroup of H.
(ii) If Q is a Sylow p-subgroup of H, there exists a Sylow p-subgroup P of G such that $Q = f(P)$.
(iii) $N_p(H) \leq N_p(G)$.

(22) Let $H \leq G$, a finite group. Let P be a Sylow p-subgroup of H. If $N_G(P) \leq H$, prove that P is a Sylow p-subgroup of G.

(23) Let $|G| = p(p+1)$. Prove that G has either a normal subgroup of order p or one of order $p+1$.
Hint: If $N_p > 1$, choose $x \in G$ of order different from 1 or p. Show that $|C_G(x)| = p+1$. Now count the elements.

(24) Let G be a finite group in which every Sylow p-subgroup is normal. If P is a Sylow p-subgroup show that $Z(P) \leq Z(G)$. Also, if N is normal in G, then $|N \cap Z(G)| > 1$.

(25) Show that the center of a group of oder 60 cannot be of order 4.

(26) Let $|G| = 60$. If Sylow p-subgroup for 3 is normal, so is Sylow p-subgroup for 5.
Hint: Let H be the Sylow 3-subgroup. If K_i, $1 \leq i \leq 6$ are the Sylow 5-subgroups, count the number of elements in K_i and the generators of HK_i. They will be $24 + 6 \times 8 > 60$ elements.

(27) Show that a group G of order 105 has a subgroup of order 35. Show that it is normal in G. Hence conclude that the Sylow subgroups of 7 and 5 are normal.
Hint: If $N_7 = 15$, there are 90 elements of order 90. The rest 15 elements come from the product of Sylow 3 and 5 subgroups. In particular, Sylow 5-subgroup is normal. Recall product of a normal subgroup and a subgroup is a subgroup. Let H be the product group, What is its index? To show the last part, compare $N_5(G)$ and $N_5(H)$ to reduce $N_5(G)$ etc. See Item 6(18)14 on page 31

(28) Let a prime p divide $|G|$. Let the Sylow p-subgroup for p is normal. Let n be the number of elements of order p. Show that p divides $n+1$.
Hint: Let $|P| = p^m$. Let n_i be the number of elements of order p^i. Then

$$n = p^m - (n_{m-1} + \cdots + n_2 + n_0).$$

Note that every summand on the right except the last term is divisible by p and $n_0 = 1$.

(29) Show that a group of order 108 has a normal subgroup of order 9 or 27.
Hint: Let P be a Sylow 3-subgroup,. Let G act on the left cosets of P. We have a homomorphism $\varphi\colon G \to S_4$ What are the possible orders of $\ker \varphi$?

13 Finite Abelian Groups

1. Let G be a finite abelian group. Let H be any subgroup of G. Then there exists a complement K such that $G = H \oplus K$.

   Let M be a subgroup such that $M \cap H = (0)$ and M is maximal with this property. We claim that $G = H \oplus M$. If not, then there exists an $x \in G \setminus (H + M)$. We may

assume that the order $o(x)$ is minimal with this property and hence is a prime. Observe that the subgroup $M+ < x >$ contains M properly and hence $M+ < x > \cap H \neq (0)$. Let $y + jx = h$. Note that $j \neq 0$. Now, $jx \in H + M$ But $< jx >=< x >$ and hence $x \in H + M$, a contradiction. □

2. **Structure Theorem for Finite Abelain Groups–Invariant Factors Form.** *Let G be a finite abelian group. Then G is a finite direct sum of cyclic groups H_i, $1 \leq i \leq r$ such that $|H_{i+1}|$ divides the order of $|H_i|$ for $1 \leq i \leq r-1$.*

   We prove this by induction on $|G| = 1$. The result is true if $|G| = 1$. Assume that the result is true for all natural numbers less than $n > 1$. Let G be a finite abelian of order $n > 1$. Let $a \in G$ be of maximal order. Let H_1 be the cyclic group generated by a. If $H_1 = G$, there is nothing to prove. If not, by the last lemma there exists a subgroup $M \leq G$ such that $GH_1 \oplus M$. Since $|M| < |G| = n$, by induction hypothesis, M is the direct sum of cyclic subgroups H_j, $2 \leq j \leq r$ where $|H_{j+1}|$ divides $|H_j|$ for $2 \leq j < r$. Assume that H_j is the cyclic subgroup generated by a_j, $2 \leq j < n$. Since a is of maximal order, it follows that $o(x)$ divides $o(a)$ for any $x \in G$. In particular, if we let $n_j := o(a_j)$ it follows that $n_r \mid n_{r-1} \mid \cdots \mid n_2 \mid n_1 := m$. The proof is complete. □

3. Let G be a finite abelian group. Let p be a prime such that the order of each element of G is of the form p^r. Then $|G|$ is of the form p^n.

   Trivial, if we use Cauchy's theorem. If q is any prime divisor (other than p) of $|G|$, then there exists an element of order q.

   We use induction to see a direct proof. If G is cyclic, then there is nothing to prove. Choose $e \neq a \in G$. Then $\langle a \rangle$ is a proper subgroup of G. The order of the quotient group $G/\langle a \rangle$ is less than $|G|$. The order of each element of $G/\langle a \rangle$ is a power of p. Hence by induction, the order of $G/\langle a \rangle$ is a power of p. Since $|G| = |G/\langle a \rangle| \times |\langle a \rangle|$, the result follows. □

4. Let G be a finite abelian group of order $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, where p_i's are distinct prime numbers. Let $G(p_i) := \{x \in G : p_i^{\alpha_i} x = 0\}$. Then each $G(p_i)$ is a p_i-subgroup of G.

   It is easy to see that this is a subgroup of G. That it is a p_i-group follows from the last item.

5. With the notation as above, we claim that each $x \in G$ can be written as $x = x_1 + \cdots + x_n$ where $x_i \in G(p_i)$, $1 \leq i \leq n$. Thus, we have $G = G(p_1) + \cdots + G(p_n)$.

   Let q_i be defined by $|G| = p_i^{\alpha_i} q_i$. That is, $q_i = p_1^{\alpha_1} \cdots \widehat{p_i^{\alpha_i}} \cdots p_n^{\alpha_n}$. Since p_i's are distinct, the q_i's have 1 as their GCD. Hence there exists m_i such that $1 = m_1 q_1 + \cdots + m_n q_n$. Hence we have

   $$x = 1 \cdot x = m_1 q_1 x + \cdots + m_n q_n x = x_1 + \cdots + x_n, \text{ where} x_i = m_i q_i x.$$

   Clearly, $p_i^{\alpha_i} x_i = m_i |G| x = 0$ and hence $x_i \in G(p_i)$.

6. The sum in the last item is direct.

   Enough to show that if $x_1 + \cdots + x_n = 0$, with $x_i \in G(p_i)$, then each $x_i = 0$. Let p_i and q_i be as earlier. Since they are relatively prime, there exists $s, t \in \mathbb{Z}$ such that

$sp_i^{\alpha_i} + tq_i = 1$. Note that $x_i = -(x_1 + \cdots + \hat{x_i} + \cdots + x_n)$. We have

$$x_i = 1 \cdots x_i = sp_i x_i + t \sum_{j \neq i} q_i x_j.$$

Since $x_i \in G(p_i)$, the first summand is zero. The presence of $p_j^{\alpha_j}$ in q_i ensures $q_i x_j = 0$ for $j \neq i$. Hence we conclude that each $x_i = 0$.

7. We have thus proved the following result known as the primary decomposition theorem:

   Theorem 6. *Let G be a finite abelian group of order $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, where p_i's are distinct prime numbers. Let $G(p) := \{x \in G : p^\alpha x = 0\}$ where p is one of the p_i's and α is the corresponding α_i.* □

8. Let G be a finite abelian p-group. Let $a \in G$ be of maximal order. Let $H := \langle a \rangle$. Then there exists a subgroup $K \leq G$ such that $G = H \oplus K$.

   To look at the nontrivial part, assume that G is not cyclic. Let $a \in G$ be of maximal order, say, p^m. We claim that there exists an element $x \in G \setminus \langle a \rangle$ of order p.

   Let $b \in G \setminus \langle a \rangle$ be of least possible order. Note that $b \neq 0$. if $pb = 0$, we are through. Assume that $\text{ord}(b) = p^r$. Consider pb. Its order is p^{r-1}. By our hypothesis on b, pb must be in $\langle a \rangle$. Thus, $pb = ka$. Hence we obtain

   $$0 = p^r b = p^{r1}(pb) = p^{r-1}(ka) = (p^{r-1}k) = a.$$

   Since $\text{ord}(a) = p^r$, it follows that p^r divides $p^{r-1}k$ and hence p divides k. Therefore, $k = pq$ for some $q \in \mathbb{Z}$. Let $c := b - qa$. Then $c \notin \langle a \rangle$ since otherwise $b = c + qa \in \langle a \rangle$, a contradiction. Also, we have

   $$pc = pb - pqa = pb - ka = 0.$$

   We conclude that $c \notin \langle a \rangle$ is of order p.

   Changing the notation, we may assume that b is of order p. Clearly, $\langle a \rangle \cap \langle b \rangle = (0)$. (For, otherwise $\langle b \rangle \subset \langle a \rangle$.) It follows that the element $a + \langle b \rangle$ is order p^m in the quotient group $G/\langle b \rangle$. By induction hypothesis, there exists a subgroup, say, $\overline{K}$ such that $G/\langle b \rangle = \langle a + \langle b \rangle \rangle \oplus \overline{K}$. Let $K \leq G$ be such that $\overline{K} = K/\langle b \rangle$.

   We claim that $G = K + H$. For, $\langle b \rangle \subset K$, we have $G = K + (\langle a \rangle + \langle b \rangle) = K + \langle a \rangle$.

   We claim that $K \cap \langle a \rangle = (0)$. If $x \in K \cap \langle a \rangle$, then $x \in K \cap (\langle a \rangle + \langle b \rangle) = \langle b \rangle$. Thus $x \in \langle a \rangle \cap \langle b \rangle = (0)$. □

9. Any finite abelian p-group is a direct sum of cyclic p-subgroups.

   Follows by induction and the last result.

10. Are the p-subgroups in the primary decomposition unique?

1. Some counting theorems such as $|AB| = \frac{|A||B|}{|A \cap B|}$, Poincare's theorem on subgroups of finite indices, Burnside lemma. Some number theoretic results such as Fermat, Wilson etc.

2. Conjugacy classes in S_n, A_n, D_{2n} and $GL(2, \mathbb{R})$.