Theorem 1. A mapping is bijective if and only if it is invertible.

Proposition 2. If $\alpha\colon S \to T$ is invertible, then there is a *unique* mapping $\beta\colon T \to S$ such that $\beta \circ \alpha = \iota_S$ and $\alpha \circ \beta = \iota_T$.

Proposition 3. Let $*$ be an operation on a set S. If S contains an identity element for $*$, then it is unique.

[In other words, the number of identity elements for $*$ in S is either 0 or 1.]

Proposition 4. Let $*$ be an associative operation on a set S, and suppose that S contains an identity element for $*$. If $x \in S$ and x is invertible with respect to $*$, then there is a *unique* element $y \in S$ such that $x * y = e$ and $y * x = e$.

Proposition 5. If α, β are disjoint cycles in S_n then $\alpha \circ \beta = \beta \circ \alpha$.

Fact 6. (a) Every permutation in S_n is the product of a finite number of disjoint cycles.

(b) Consequently, every permutation in S_n is the product of a finite number of transpositions.

Theorem 7. If $\alpha, \beta \in S_n$ then $\sigma(\alpha \circ \beta) = \sigma(\alpha)\sigma(\beta)$.

Proposition 8. If $a_1, \ldots, a_k$ are distinct integers and $k \geq 2$, then

$$\sigma\big((a_1\ a_2\ \ldots\ a_k)\big) = (-1)^{k-1}.$$

Definition. If $(G, *)$ is a group and $H \subseteq G$, then H is a *subgroup* of $(G, *)$, or $H \leq G$, or $H \leq (G, *)$, if:

(SG0) $H \neq \emptyset$

(SG1) $x, y \in H \implies x * y \in H$

(SG2) $x \in H \implies x^{-1} \in H$

Theorem 9. Let $(G, *)$ be a group with identity element e, and let H be a subgroup of G.

(a) The mapping $*_H \colon H \times H \to H$ given by $x *_H y = x * y$ for $x, y \in H$ is a well-defined operation on H such that $(H, *_H)$ is a group.

(b) $e \in H$, and e is the identity element of $(H, *_H)$

(c) if $x \in H$, then the inverse of x with respect to $*$ is the same as the inverse of x with respect to $*_H$.

Lemma 10. If $(G, *)$ is a group with identity element e, then $e^{-1} = e$.

Theorem 11. If $(G, *)$ is a group and H is a non-empty subset of G, then H is a subgroup of $(G, *)$ if and only if

$$x, y \in H \implies x * y^{-1} \in H.$$

Theorem 12. $A_n = \{\alpha \in S_n \colon \alpha \text{ is an even permutation}\}$ is a subgroup of $(S_n, \circ)$.

Theorem 13. Let S be a set and let $(G, \circ)$ be a group of bijections $S \to S$ (so that G is a subgroup of $(\mathrm{Sym}(S), \circ)$). If $T \subseteq S$, then

$$G_T = \{\alpha \in G \colon t \in T \implies \alpha(t) = t\}$$

is a subgroup of $(G, \circ)$.

Lemma 14. Let S be a set, let $\alpha \colon S \to S$ be a bijection and let $T \subseteq S$. Then $\alpha(T) = T \implies \alpha^{-1}(T) = T$.

Theorem 15. Let S be a set and let $(G, \circ)$ be a group of bijections $S \to S$ (so that G is a subgroup of $(\mathrm{Sym}(S), \circ)$). If $T \subseteq S$, then

$$G_{(T)} = \{\alpha \in G \colon \alpha(T) = T\}$$

is a subgroup of $(G, \circ)$.

Theorem 16. If M is the set of motions (distance preserving bijections) of the plane P, then M is a subgroup of $(\mathrm{Sym}(P), \circ)$.

Lemma 17. If $\alpha \in M$ and $\alpha(0) = 0$, $\alpha(e_1) = e_1$ and $\alpha(e_2) = e_2$, then $\alpha = \iota_P$. [Here, $e_1 = \binom{1}{0}$ and $e_2 = \binom{0}{1}$.]

Theorem 18. Every motion $\alpha \in M$ can be written as either

$$\alpha = \tau_a \circ \rho_\theta \quad \text{or} \quad \alpha = \tau_a \circ \rho_\theta \circ r$$

for some $a \in P$ and some $\theta \in \mathbb{R}$, where

- $\tau_a \colon P \to P$, $p \mapsto p + a$ is translation by a,
- $\rho_\theta \colon P \to P$, $p \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} p$ is rotation by θ about 0, and
- $r \colon P \to P$, $\binom{x}{y} \mapsto \binom{x}{-y}$ is reflection in the x-axis.

Theorem 19. Let S be a non-empty set.

(a) If $\sim$ is an equivalence relation on S, then the collection of its equivalence classes is a partition of S.

(b) If $\mathscr{P}$ is a partition of S, then the relation $\sim$ on S defined by

$$x \sim y \iff \exists\, A \in \mathscr{P} \colon x \in A \text{ and } y \in A$$

is an equivalence relation on S.

Theorem 20. Let G be a permutation group on a set S. The relation $\sim$ on S defined by

$$x \sim y \iff \exists\, \alpha \in G \colon \alpha(x) = y$$

is an equivalence relation on S. (It's called *G-orbit equivalence*).

Theorem 21. Let $n \in \mathbb{N}$. The relation on $\mathbb{Z}$ of *congruence modulo n* defined for $a, b \in \mathbb{Z}$ by

$$a \equiv b \pmod{n} \iff n \mid a - b$$

is an equivalence relation on $\mathbb{Z}$.

Theorem 22 (The division algorithm)**.** Let $n \in \mathbb{N}$. For every integer a, there exist unique integers q, r with $0 \leq r < n$ such that $a = qn + r$. That is,

$$\forall\, a \in \mathbb{Z},\ \exists!\, q \in \mathbb{Z} \text{ and } r \in \{0, 1, \ldots, n-1\} \colon\ a = qn + r.$$

Corollary 23. Let $n \in \mathbb{N}$. The set $\{0, 1, \ldots, n-1\}$ is a complete set of equivalence class representatives for the equivalence relation of congruence modulo n.

Theorem/Definition 24. Let $n \in \mathbb{N}$. There is a well-defined operation $\oplus \colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ given by $[k] \oplus [\ell] = [k + \ell]$ for $k, \ell \in \mathbb{Z}$. Moreover, $(\mathbb{Z}_n, \oplus)$ is an abelian group, called the *group of integers modulo n*.

Corollary 25. For all $n \in \mathbb{N}$, there is an abelian group of order n.

Fact/Definition 26. If a, b are non-zero integers then there is a unique $d \in \mathbb{N}$ such that

- $d|a$ and $d|b$
  ["d is a common divisor of a and b"], and
- if $c \in \mathbb{Z}$ with $c|a$ and $c|b$, then $c|d$
  ["every common divisor of a and b divides d"]

In symbols:

$$\forall\, a, b \in \mathbb{Z} \setminus \{0\}\ \ \exists!\, d \in \mathbb{N} \colon \begin{cases} d|a \text{ and } d|b, \text{ and} \\ [\, c \in \mathbb{Z} \colon\ c|a \ \text{ and } c|b\,] \implies c|d. \end{cases}$$

We call d the *greatest common divisor of a and b*, and write this as $\gcd(a, b)$ or (a, b).

Theorem 27. Let G be a group and let $a, b, c \in G$.

(a) $ab = ac \implies b = c$ [left cancellation]

(b) $ba = ca \implies b = c$ [right cancellation]

(c) $\exists! \, x \in G : ax = b$, and $\exists! \, y \in G : ya = b$

(d) $ab = e \implies b = a^{-1}$, and $ba = e \implies b = a^{-1}$

(e) $(c^{-1})^{-1} = c$

(f) $(ab)^{-1} = b^{-1}a^{-1}$

Definition. Let G be a group with identity element e, let $a \in G$ and let $n \in \mathbb{Z}$. We define

$$a^n = \begin{cases} \underbrace{a \cdots a}_{n \text{ times}} & \text{if } n > 0 \\ e & \text{if } n = 0 \\ \underbrace{a^{-1} \cdots a^{-1}}_{-n \text{ times}} & \text{if } n < 0 \end{cases}$$

and note that $a^n a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$ for all $n, m \in \mathbb{Z}$.

Theorem 28. Let a be an element of a group G. Let $\langle a \rangle$ be the set of all integer powers of a, so that $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$. Then $\langle a \rangle$ is a subgroup of G.

We call such a subgroup a *cyclic subgroup* of G.

If $G = \langle a \rangle$ for some $a \in G$, we say G is a *cyclic group*.

Proposition 29. $\langle a \rangle$ is an abelian subgroup of G. In particular, if G is cyclic then G is abelian.

Definition. Let G be a group with identity element e and let a be an element of G. Consider $S = \{k \in \mathbb{N} : a^k = e\}$. We define the *order of* a as

$$o(a) = \begin{cases} \text{the least element of } S & \text{if } S \neq \emptyset \\ \infty & \text{if } S = \emptyset. \end{cases}$$

Theorem 30. If $o(a) \neq \infty$ and $n = o(a)$ then

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$

and $a^r \neq a^s$ if $r, s \in \mathbb{Z}$ with $0 \leq r, s < n$ and $r \neq s$, so $|\langle a \rangle| = n$.

Theorem 31. If $o(a) = \infty$ then

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, a^4, \ldots\}$$

and $a^r \neq a^s$ if $r, s \in \mathbb{Z}$ with $r \neq s$, so $|\langle a \rangle| = \infty$.

Corollary 32. $|\langle a \rangle| = o(a)$ for any $a \in G$.

Definition. Let G and H be two groups. The set

$$G \times H = \{(g, h) : g \in G,\ h \in H\}$$

together with the operation on $G \times H$ defined by

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2) \quad \text{for } g_1, g_2 \in G \text{ and } h_1, h_2 \in H$$

is called the *direct product* of G and H.

Theorem 33. The direct product of two groups is a group.
If G and H are finite groups then the order of $G \times H$ is $|G| \cdot |H|$.
If either G or H is infinite, then so is $G \times H$.

Let H be a subgroup of a group G.

Definition. If $a \in G$, the *(right) coset* of H by a is the set

$$Ha \stackrel{\text{def}}{=} \{ha\colon\ h \in H\}.$$

[Here, a is fixed and h is a dummy variable.]

The (right) cosets of H in G are the sets Ha for $a \in G$.

Theorem 34. The relation $\sim$ on G defined by

$$a \sim b \iff ab^{-1} \in H \quad \text{for } a, b \in G$$

is an equivalence relation.

Theorem 35. If $b \in G$ then $[b]_\sim = Hb$. So the equivalence classes for $\sim$ are the same as the right cosets of H in G.

Moreover, the following conditions are equivalent:

(a) $ab^{-1} \in H$

(b) $a = hb$ for some $h \in H$

(c) $a \in Hb$

(d) $Ha = Hb$

Lemma 36. If G is a group and H is a subgroup of G, then $|H| = |Ha|$ for every $a \in G$.

Theorem 37 (Lagrange's theorem)**.**
If G is a finite group and H is a subgroup of G, then $|H| \Big| |G|$.

Corollary 38. Let G be a finite group with identity element e. For every $a \in G$, we have $o(a) \Big| |G|$ and, in particular, $a^{|G|} = e$.

Corollary 39. Let G be a finite group with identity element e. If $|G|$ is a prime number, then

(a) the only subgroups of G are $\{e\}$ and G; and

(b) G is a cyclic group, and $G = \langle a \rangle$ for every $a \in G$ with $a \neq e$.

Theorem 40. Let G and H be two groups, and let $\theta : G \to H$ be a homomorphism. Then

(a) $\theta(e_G) = e_H$;

(b) $\theta(a^{-1}) = \theta(a)^{-1}$ for all $a \in G$; and

(c) $\theta(a^k) = \theta(a)^k$ for all $k \in \mathbb{Z}$ and all $a \in G$.

Theorem 41. If $G \approx H$, then

(a) G is abelian $\iff$ H is abelian;

(b) $|G| = |H|$;

(c) G is cyclic $\iff$ H is cyclic; and

(d) G contains an element of order n
$\iff$ H contains an element of order n.

Theorem 42.
If G is a finite cyclic group of order n, then $G \approx \mathbb{Z}_n$.

Corollary 43.
If G and H are finite cyclic groups with $|G| = |H|$, then $G \approx H$.

Corollary 44. Let p be a prime number.
If G is a group with $|G| = p$ then $G \approx \mathbb{Z}_p$.

Theorem 45. Let G and H be two groups, and let $\theta\colon G \to H$ be a homomorphism.

(a) $\theta(G)$ is a subgroup of H

(b) $\ker\theta$ is a subgroup of G

(c) θ is injective $\iff \ker\theta = \{e_G\}$

Theorem 46. If $\theta\colon G \to H$ is an injective homomorphism, then $G \approx \theta(G)$.

Definition. If G is a group, then we write $N \lhd G$ and say that N is a *normal subgroup* of G if

- N is a subgroup of G, and
- $g \in G,\ n \in N \implies gng^{-1} \in N$.

Theorem 47. If $\theta\colon G \to H$ is a homomorphism, then $\ker\theta \lhd G$.

Theorem/Definition 48. Let G be a group and let $N \lhd G$. Let

$$G/N = \{Na\colon\ a \in G\}$$

be the set of all right cosets of N in G. There is a well-defined operation on G/N given by

$$(Na)(Nb) = N(ab)$$

and this operation turns G/N into a group. The identity element of G/N is $e_{G/N} = N$ and the inverse of Na is $(Na)^{-1} = N(a^{-1})$.

Theorem 49 (The Fundamental Homomorphism Theorem)**.** Let G and H be groups, and let $\theta\colon G \to H$ be a surjective homomorphism, and let $K = \ker\theta$. Then $G/K \approx H$, and in fact

$$\phi\colon G/K \to H, \qquad \phi(Ka) = \theta(a) \quad \text{for } a \in G$$

is a well-defined isomorphism.

Corollary 50. Let G and H be groups, and let $\theta\colon G \to H$ be a homomorphism, and let $K = \ker\theta$. Then $G/K \approx \theta(G)$, and in fact

$$\phi\colon G/K \to \theta(G), \qquad \phi(Ka) = \theta(a) \text{ for } a \in G$$

is a well-defined isomorphism.