MA3K4 Introduction to group theory :: Lecture notes

Lecturer: Gareth Tracey

October 13, 2023

Contents

Week 1, lecture 1 starts here

1 Introduction

Definition 1.0.1. A *group* is a pair $(G, \circ)$ where G is a set and $\circ : G \times G \to G$ is a binary operation satisfying

1. Associativity: $(g \circ h) \circ k = g \circ (h \circ k)\ \forall g, h, k \in G$,
2. Identity: $\exists$ an element in G, denoted 1_G, such that $1_G \circ g = g \circ 1_G = g\ \forall g \in G$,
3. Inverses: $\forall g \in G$, $\exists$ an element in G, denoted g^{-1}, such that $g \circ g^{-1} = g^{-1} \circ g = 1_G$.

Remark. Implicit in parts 1 and 2 of above definition are

1. An identity element in an associative binary operation is unique, justifying the notation and the 'the' before 'identity'
2. Similarly, inverses are unique in an associative binary operation, so we say *the* inverse of g

The number of elements in a group $(G, \circ)$ is called the order of G, denoted $|G|$.

Example 1.0.2. Let $G = \mathbb{Z}$. Then

1. If we define $\circ : G \times G \to G$ by $g \circ h = g + h$ for $g, h \in \mathbb{Z}$ then we know $(G, \circ)$ is a group and $1_G = 0,\ g^{-1} = -g\ \forall g \in G$.
2. For the same set, if we define $g \circ h = g \times h$ then $(G, \circ)$ is not a group for lack of inverses for $g \in \mathbb{Z} \backslash \{\pm 1\}$.

Remark. 1. You may have been given a fourth axiom, closure, in previously seen definitions of a group. The reason we omit that here is because it's implied by definition of binary operation.

2. If $(G, \circ)$ is a group, $\circ$ is often called the *group operation*.
3. Given clear context, we will streamline our notation and simply write G in place of $(G, \circ)$ and gh in place of $g \circ h$.

Definition 1.0.3. Let G be a group.

1. If $g, h \in G : gh = hg$ then g and h *commute*.
2. If g and h commute $\forall g, h \in G$ then G is *abelian*.

Example 1.0.4. $(\mathbb{Z}, +)$ is abelian.

Exercise 1.0.5 (Commuting elements in groups)**.** Let G be a group.

1. Suppose $g^2 = 1_G\ \forall g \in G$. Show that G is abelian.

   Proof. Note that this implies $\forall g, h \in G,\ (gh)^{-1} = gh$, but $(gh)^{-1} = h^{-1}g^{-1} = hg$, so $gh = hg$. □

2. Suppose $g^3 = 1_G\ \forall g \in G$. Show that hgh^{-1} and g commute $\forall g, h \in G$.

   Proof. One has $g^2h = g^{-1}h^{-2} = (h^2g)^{-1} = h^2gh^2g \Rightarrow gh^2g = hg^2h \Rightarrow hgh^2g = h^2g^2h$. Now consider $(gh)^{-1}$, which equals h^2g^2 but also $ghgh$. Hence $ghgh^{-1} = ghgh^2 = h^2g^2h = hgh^2g = hgh^{-1}g$, as desired. □

Next, we are going to look at two infinite families of examples of groups: 1. Symmetric groups and 2. Linear groups.

1.1 Symmetric group

Definition 1.1.1. Let X be a set, and define

$$\mathrm{Sym}(X) = \{f : f : X \to X \text{ is a bijection}\}$$

Define $\circ : \mathrm{Sym}(X) \times \mathrm{Sym}(X) \to \mathrm{Sym}(X)$ to be the usual composition of functions. Then $(\mathrm{Sym}(X), \circ)$ is a group, called the *symmetric group* on X. An element of $\mathrm{Sym}(X)$ is called a *permutation.*

Remark (Sanity check)**.**
1. Associativity is clear by inheritance
2. $1_G = \mathrm{id}_X : x \mapsto x$
3. For $f \in \mathrm{Sym}(X)$, $x \in X$, choose a unique $y_x \in X$ such that $f(y_x) = x$. Define $g : X \to X$ by $g(x) = y_x$, then g is a inverse for f.

We introduce cycle notation as a more compact way of writing permutations down.

Week 1, lecture 2 starts here

Definition 1.1.2 (Cycle notation)**.** Let X be a set.

1. Let $a_1, \ldots, a_n \in X$ be distinct. The permutation $f = (a_1, \ldots, a_n) \in \mathrm{Sym}(X)$ is defined to be $f(a_i) = a_{i+1}$ for $1 \leq i \leq n-1$, $f(a_n) = a_1$, and $f(b) = b$ for $b \notin \{a_1, \ldots, a_n\}$. We call f a *cycle of length* n (or an n-cycle).
2. Two cycles $(a_1, \ldots, a_r)$, $(b_1, \ldots, b_s)$ are *disjoint* if $\{a_1, \ldots, a_r\} \cap \{b_1, \ldots, b_s\} = \varnothing$.
3. The *empty cycle*, written $()$, is the identity map which is also $1_{\mathrm{Sym}(X)}$.

Remark (Important points about cycles)**.**
1. Perhaps a tautology, but the empty cycle is thought of as a cycle (of lenght 0).
2. Recall that the group operation is composition of functions. So $fg : X \to X$ means do g first and then f. e.g. $X = \{1, 2, 3, 4, 5\}$, so $(3, 4, 1, 2)(4, 5) = (1, 2, 3, 4, 5)$.
3. Cycle notation is not unique in the following sense: two distinct m-tuples of elements in a set X can represent the same cycle, e.g. $(1, 2, 3, 4, 5) = (3, 4, 5, 1, 2)$.

Theorem 1.1.3. Let X be a finite set. Then

1. $|\mathrm{Sym}(X)| = |X|!$,

2. Every element $F \in \mathrm{Sym}(X)$ can be written as product of disjoint cycles. Moreover, the decomposition is unique in the sense that if $F = f_1 \cdots f_r = g_1 \cdots g_s$ where f_i, g_i are disjoint cycles of length > 1, then $r = s$ and $\{f_1, \dots, f_r\} = \{g_1, \dots, g_r\}$.

Proof (nonexaminable). 1. Write $X = \{x_1, \dots, x_r\}$ where $n = |X|$ and define

$$X(n) := \{(a_1, \dots, a_n) : a_i \in X, a_i \neq a_j \text{ for } i \neq j\}.$$

Define a bijection $\theta : \mathrm{Sym}(X) \to X(n)$ by $\theta(f) = (f(x_1), \dots, f(x_n))$. for $f \in \mathrm{Sym}(X)$, observe

(a) θ is well-defined, since f is a bijection, so $f(x_i) \neq f(x_j)$ for $i \neq j$.

(b) In the same way, θ is injective. Indeed, if $\theta(f) = \theta(g)$ then $f(x_i) = g(x_i)$ $\forall i$ by definition of θ, so $f = g$.

(c) If $(a_1, \dots, a_n) \in X(n)$, then define $f : X \to X$ by $f(x_i) = a_i$ for $1 \leq i \leq n$. Clearly, $f \in \mathrm{Sym}(X)$ and $\theta(f) = (a_1, \dots, a_n)$, so θ is surjective.

It follows that $|\mathrm{Sym}(X)| = |X(n)| = n!$.

2. Let $f \in \mathrm{Sym}(X)$. If $f = \mathrm{id}_X$ then $f = ()$ so it's a cycle. Now suppose f is not id_X. Let $Y = \{x \in X : f(x) \neq x\}$. Note that since $|\mathrm{Sym}(X)|$ is finite by 1., $\exists n \in \mathbb{N}$ such that $f^n = \mathrm{id}_X$.

   In particular, if we fix $a_1 \in Y$, then we may define $m_1 := \min\{m \in \mathbb{N} : f^m(a_1) = a_1\}$ since the set is nonempty. Now, for $2 \leq i \leq m_1$, define $a_i := f(a_{i-1})$. If $Y = \{a_1, \dots, a_{m_1}\}$, then by definition of cycle, one has $f = (a_1, \dots, a_m)$.

   Now suppose $Y \backslash \{a_1, \dots, a_{m_1}\} \neq \varnothing$. Choose $a_{m_1+1} \in Y \backslash \{a_1, \dots, a_{m_1}\}$, and define $m_2 := \min\{m \in \mathbb{N} : f^m(a_{m_1+1}) = a_{m_1+1}\}$. For $m_1 + 2 \leq i \leq m_2$, again define $a_i := f(a_{i-1})$, then if $Y = \{a_1, \dots, a_{m_1}, a_{m_1+1}, \dots, a_{m_2}\}$, one has $f = (a_1, \dots, a_m)(a_{m+1}, \dots, a_{m_2})$. If not, we continue inductively. Since X is finite, this must terminate, and when it does f will be a product of disjoint cycles. The uniqueness follows from the algorithm immediately.

□

1.2 Linear group

Definition 1.2.1. F is a field and $n \in \mathbb{N}$. We define

$$GL_n(F) := \{A : A \text{ an invertible } n \times n \text{ matrix over } F\},$$

a group with matrix multiplication as operation. This is called *general linear group* of dimension n over F.

Week 1, lecture 3 starts here

Remark (Useful things from Algebra I, II for studying general linear groups). 1. Each field F has an additive and multiplcative identity 0_F and 1_F. Given clear context, they will be denoted simply 0 and 1 respectively.

2. An $n \times n$ matrix A over F is invertible iff $\det A \neq 0$ iff rows (or columns) of A are linearly independent.

3. If F is a finite field, then $|F| = p^f$ for some prime p and $f \in \mathbb{N}$. Moreover, for each prime p and each $f \in \mathbb{N}$, $\exists!$ a field (up to isomorphism) $F : |F| = p^f$. p is called the *characteristic* of F, and satisfies that $p\alpha = 0\ \forall \alpha \in F$.

4. If F is a field then $F^\times := F \backslash \{0\}$ is a group with multiplication as group operation inherited from F.

Exercise 1.2.2. 1. Let X be a set. Show that $\mathrm{Sym}(X)$ is abelian iff $|X| \leq 2$.

2. Let F be a field. Show that $GL_n(F)$ is abelian iff $n = 1$.

Theorem 1.2.3. Let F be a finite field with $|F| = q$. Then $|GL_n(F)| = q^{\binom{n}{2}} \prod_{i=1}^{n} (q^i - 1)$.

Proof (nonexaminable). See exercise sheet 1. $\square$

1.3 Order of elements

Definition 1.3.1. The *order* of $g \in G$, denoted $|g|$, is defined $|g| := \min\{n \in \mathbb{N} : g^n = 1_G\}$. If the set is $\varnothing$ then $|g| := \infty$.

Example 1.3.2. 1. Let X be a set and let $f = (a_1, \ldots, a_m) \in \mathrm{Sym}(X)$. Then $|f| = m$.

2. Let F be a finite field of order p^f where p prime, $G = GL_2(F)$, and $\alpha, \beta \in F^\times$. Observe that
$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha + \beta \\ 0 & 1. \end{pmatrix}$$
So if $g = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ then $g^n = \begin{pmatrix} 1 & n\alpha \\ 0 & 1 \end{pmatrix}$, so $|g| \mid p$ (we'll see later about this implication), so $|g| = p$.

   Also,
$$g^n = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}^n = \begin{pmatrix} \alpha^n & 0 \\ 0 & \beta^n. \end{pmatrix}$$
So $|g| = \mathrm{lcm}\ (m, k)$ where $m = |\alpha|$ and $k = |\beta|$ as elements of $F^\times$.

Remark. 1. For $g \in G$, $(g^n)^{-1} = \left(g^{-1}\right)^n$, so we write $g^{-n} := \left(g^{-1}\right)^n$. In particular, $\left|g^{-1}\right| = |g|$.

2. If $g \in G$, $n = |g|$ and $n \mid l$, then $g^l = 1$.

Lemma 1.3.3. Let $a, b \in G$ of finite order. Then

1. If $l \in \mathbb{N}$, then $a^l = 1$ iff $|a| \mid l$.

2. Let $m \in \mathbb{N}$, then $|a^m| = \dfrac{|a|}{\gcd(|a|, m)}$.

3. If a, b commute then $|ab| \mid \mathrm{lcm}\ (|a|, |b|)$.

4. If a, b commute and $a^i = b^j\ \forall i, j \in \mathbb{N}$ only when they are both 1 (i.e. $\langle a \rangle \cap \langle b \rangle = \{1\}$) then $|ab| = \mathrm{lcm}\ (|a|, |b|)$.

Proof. 1. $\Leftarrow$ is mentioned. $\Rightarrow$: suppose $a^l = 1$. By Euclidean division, we can write $l = q|a|+r$ for some $r \in [0, |a|)$. Then $1 = a^l = a^{q|a|+r} = a^r$, which contradicts minimality of $|a|$.

2. Suppose first that $m \mid |a|$. Then one can write $|a| = ms$, so $a^{ml} = 1 \Leftrightarrow |a| \mid ml$ by 1 $\Leftrightarrow \dfrac{|a|}{m} \mid l$. Hence the least positive integer $l : a^{ml} = 1$ is $\dfrac{|a|}{m}$.

   Now let $k = \gcd(|a|, m)$. We write $m = ks$, then $a^{m\frac{|a|}{k}} = a^{|a|s} = 1$, and by 1 one has $|a^m| \mid \frac{|a|}{k}$. To complete the proof it suffices to show that $\frac{|a|}{k} \leq |a^m|$.

   Week 2, lecture 1 starts here

   By Bézout's lemma, $\exists s, t \in \mathbb{Z} : k = s|a| + tm$, so $a^k = a^{s|a|+tm} = (a^{|a|})^s a^{tm} = a^{tm}$. Then $a^{tm|a^m|} = ((a^m)^{|a^m|}))^t = 1^t = 1$. This implies $|a^{tm}| \mid a^m$ by 1. So $\frac{|a|}{k} = |a^k| = |a^t m| \mid |a^m|$.

3. Let $l := \text{lcm}\ (|a|, |b|)$. Then $(ab)^l = a^l b^l = 1 \times 1 = 1$, so by 1. $|ab| \mid l$.

4. Let $k := |ab|$. Then $k \mid l$, but also, $1 = (ab)^k = a^k b^k$ so $a^k = \left(b^{-1}\right)^k$ and by assumption both sides are 1. So $|a|, |b| \mid k$, so $l \mid k$, hence $k = l$.

$\square$

Exercise 1.3.4. 1. Let $h, g \in G$. Show that $\left|hgh^{-1}\right| = |g|$.

2. Let $l, m, n > 2 \in \mathbb{N}$. Show that $\exists G$ with $a, b \in G : |a| = l,\ |b| = m,\ |ab| = n$. Also:

   (a) Show that G can be finite.

   (b) Show that one can replace $l, m, n > 2$ by $l, m, n > 1$.

   Key hint: A 2×2 matrix over $\mathbb{C}$ with distinct eigenvalues is diagonalisable. Now exploit result of 1st exercise.

1.4 Subgroup and coset

Definition 1.4.1. A nonempty $H \subseteq G$ is a *subgroup* of G, denoted $H \leq G$, if

1. $1_G \in H$
2. $h \in H \Rightarrow h^{-1} \in H$
3. $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$

Definition 1.4.2. For a group G and $g \in G$, define $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$ which is called the *cyclic subgroup of G generated by g*. If $G = \langle g \rangle$ then G is *cyclic* and g is a *generator* for G.

Lemma 1.4.3. $H \subseteq G$ where H nonempty. $H \leq G \Leftrightarrow h_1 h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$

Proof. $\Rightarrow$ $h_1, h_2 \in H \Rightarrow h_2^{-1} \in H \Rightarrow h_1 h_2^{-1} \in H$.

$\Leftarrow$
1. $H \neq \varnothing \Rightarrow h \in H \Rightarrow hh^{-1} \in H \Rightarrow 1_G \in H$
2. $h \in H \Rightarrow 1_G h^{-1} = h^{-1} \in H$
3. $h_1, h_2 \in H \Rightarrow h_2^{-1} \in H \Rightarrow h_1 (h_2^{-1})^{-1} h_1 h_2 \in H$

$\square$

Example 1.4.4. Let $G = GL_2(F)$ and

$$H = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} : \alpha, \beta \in F^\times \right\} \subseteq G. \qquad \text{sometimes called diagonal subgroup}$$

We want to show this is indeed a subgroup. Let $h_i = \begin{pmatrix} \alpha_i & 0 \\ 0 & \beta_i \end{pmatrix} \in H$ where $i = 1, 2$. Then

$$h_1 h_2 = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \beta_2 \end{pmatrix} \begin{pmatrix} \alpha_2^{-1} & 0 \\ 0 & \beta_2^{-1} \end{pmatrix} = \begin{pmatrix} \alpha_1 \alpha_2^{-1} & 0 \\ 0 & \beta_1 \beta_2^{-1} \end{pmatrix} \in H.$$

Definition 1.4.5. Let $A \subseteq G$ be nonempty. The *subgroup of G generated by A*, denoted $\langle A \rangle$, is

$$\{a_1^{\varepsilon_1} \cdots a_m^{\varepsilon_m} : m \in \mathbb{N},\ a_i \in A,\ \varepsilon_i = \{\pm 1\}\}.$$

Notation. If $A = \{g_1, \dots, g_t\}$ then we often write $\langle A \rangle$ as $\langle g_1, \dots, g_t \rangle$.

Week 2, lecture 2 starts here

Exercise 1.4.6. Let G be a group and $A \subseteq$ nonempty.

1. Use Lemma 1.4.3 to show that $\langle A \rangle$ is indeed a subgroup of G.
2. Write $A = \{g_1, \dots, g_s\}$ and suppose $g_i g_j = g_j g_i\ \forall i, j = 1, \dots, s$. Show that $|\langle A \rangle| \leq \prod_{i=1}^s |g_i|$.
3. Suppose $g^p = 1\ \forall g \in G$ and $G = \langle x, y \rangle$ for some $x, y \in G$.
   (a) Show that if $p = 2,\ |G| \leq 4$.
   (b) Show that if $p = 3,\ |G| \leq 3^4$.
   (c) Fields-medal-worth: If $p = 5$, is G finite?

Definition 1.4.7. The *left coset* of $H \leq G$ with respect to $g \in G$ is the set $gH := \{gh : h \in H\}$. The *right coset* is defined similarly.

gH is not a subgroup unless $g \in H$ since in general the identity is not there.

Lemma 1.4.8. Let $H \leq G$ and $g, k \in G$. The following are equivalent:

1. $k \in gH$
2. $kH = gH$
3. $g^{-1}k \in H$

Proof. First note that if $h \in H$ then $hH = H$ by virtue of the fact $H \leq G$.
Now $k \in gH \Rightarrow k = gh$ for some $h \in H \Rightarrow kH = ghH = gH$, so 1 implies 2. The other two implications are almost identical. □

Lemma 1.4.9. Let $H \leq G$. For $g_1, g_2 \in G$, say that $g_1 \sim_H g_2 \Leftrightarrow g_1 H = g_2 H$. Then $\sim_H$ is an equivalence relation.

Proof. The three conditions reflexivity, symmetry and transitivity follow immediately from definition. □

Corollary 1.4.10. Let $H \leq G$.

1. If $g_1, g_2 \in G$, then either $g_1 H = g_2 H$ or $g_1 H \cap g_2 H = \varnothing$.
2. The set $\{gH : g \in G\}$ of left cosets is a partition of G, i.e. if $g_i H$ for $i \in I$ are distinct left cosets of H in G then
$$G = \bigsqcup_{i \in I} g_i H.$$

Proof. $\{gH : g \in G\}$ is precisely the set of equivalence classes under $\sim_H$, so the results follow immediately. □

Theorem 1.4.11 (Lagrange's)**.** Let G be a finite group and $H \leq G$. Then $|H| \mid |G|$.

Proof. Let $g_1 H, \ldots, g_t H$ be distinct left cosets of H in G. By Corollary 1.4.10,
$$|G| = \left| \bigsqcup_{i=1}^{t} g_i H \right| = \sum_{i=1}^{t} |g_i H|,$$
and one also has $|gH| = |H| \ \forall g \in G$ since $gH \to H$ defined by $gh \mapsto h$ is a bijection. Hence $|G| = t|H|$. □

Definition 1.4.12.

1. As in the context of above, we write $G/H := \{gH : g \in G\}$.
2. $|G/H|$ is called *index* of H in G, denoted $|G : H|$. By Lagrange's theorem if G is finite then $|G : H| = \frac{|G|}{|H|}$.

Corollary 1.4.13. If G is finite and $g \in G$, then $|g| \mid |G|$.

Proof. This follows from the fact $|\langle g \rangle| = |g|$ and Lagrange's theorem. □

1.5 Normal subgroup and quotient group

In general G/H is not a group, which is the motivation of this section.

Lemma 1.5.1. Let $H \leq G,\ g \in G$. Then $gHg^{-1} = \left\{ ghg^{-1} : h \in H \right\} \leq G$.

Proof. We use Lemma 1.4.3. Clearly $gHg^{-1} \neq \varnothing$ since $1_G \in gHg^{-1}$. Now let $x = gh_1g^{-1},\ y = gh_2g^{-1}$ where $h_1, h_2 \in H$. Note that $h_1h_2 \in H$ since $H \leq G$. Then $y^{-1} = gh_2^{-1}g^{-1}$ so
$$xy^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = gh_1h_2^{-1}g^{-1} \in gHg^{-1}.$$
□

Definition 1.5.2.

1. $H \leq G$ is *normal* in G if $gHg^{-1} = H \ \forall h \in H$, denoted $N \trianglelefteq G$.
2. The *normaliser* of $H \leq G$ is defined as
$$N_G(H) := \{g \in G : gHg^{-1} = H\}.$$

Exercise 1.5.3.

1. If $H \leq G$, show that $N_G(H) \leq G$.
2. $\{1_G\}, G$ are always normal.

Week 2, lecture 3 starts here

Definition 1.5.4. G is *simple* if $\{1_G\}$ and G are the only normal subgroups of G.

Example 1.5.5.
- $\mathbb{Z}/p\mathbb{Z}$ for any prime p (by Lagrange's)
- A_n for $n \geq 5$

Notation. $AB := \{ab : a \in A, b \in B\}$ where $A, B \subseteq G$. It's a subset but not a subgroup of G in general, even if $A, B \leq G$.

Lemma 1.5.6. Let $N \trianglelefteq G$ and $g, h \in G$. Then $(gN)(hN) = ghN$.

Proof. $\subseteq$: Let $x = gn_1 \in gN,\ y = hn_2 \in hN$ where $n_{1,2} \in N$. Then

$$xy = gn_1hn_2 = ghh^{-1}n_1hn_2 \in ghN$$

since $h^{-1}n_1h \in N$ by definition of a normal subgroup.

$\supseteq$: Let $x = ghn \in ghN$ where $n \in N$. Then

$$x = (g1_G)(hn) \in (gN)(hN).$$

□

Definition 1.5.7. Let $N \trianglelefteq G$.

1. The *natural binary operation* on G/N is $\circ : G/N \times G/N \to G/N$ given by $(gN) \circ (hN) = ghN$.
2. $(G/N, \circ)$ is a group, called the *quotient of G by N*.

Checking this is indeed a group is left as an exercise.

1.6 Homomorphisms

Definition 1.6.1.
1. A map $\theta : G \to H$ is a *homomorphism* if $\theta(g_1g_2) = \theta(g_1)\theta(g_2)\ \forall \theta_{1,2} \in G$.
2. A bijective homomorphism is an *isomorphism.* If for $G, H,\ \exists\theta : G \to H$ an isomorphism, then G and H are *isomorphic*, denoted $G \cong H$.
3. Let $\theta : G \to H$ be a homomorphism. The *kernel* of θ, denoted $\ker\theta$, is defined to be $\{g \in G : \theta(g) = 1_H\}$, which is a subgroup of G. The *image* of θ, denoted im θ, is defined to be $\{\theta(g) : g \in G\}$.

Example 1.6.2. Let F be a field, $G = GL_n(F)$ and $H = F^\times$. Then $\det G \to H$ is a (surjective) homomorphism, since $\det AB = \det A \det B\ \forall A, B \in GL_n(F)$. Also

$$\ker\det = \{A \in GL_n(F) : \det A = 1_F\} =: SL_n(F).$$

Theorem 1.6.3 (1st isomorphism theorem)**.** Let $\theta : G \to H$ be an homomorphism. Then

1. $\ker\theta \trianglelefteq G$.
2. im $\theta \leq H$.

3. $G/\ker\theta \cong \mathrm{im}\ \theta$.

Theorem 1.6.4 (2nd isomorphism theorem)**.** Let $H \leq G$ and $N \trianglelefteq G$. Then

1. $HN = NH \leq G$.
2. $H \cap N \trianglelefteq H$.
3. $HN/N \cong H/(H \cap N)$.

Theorem 1.6.5 (3rd isomorphism theorem)**.** Let $N, K \trianglelefteq G : N \leq K$. Then

$$(G/N)/(K/N) \cong G/K.$$

Theorem 1.6.6 (Correspondence (or 4th isomorphism) theorem)**.** Let $N \trianglelefteq G$. Then the map

$$f : \{J : N \leq J \leq G\} \to \{X : X \leq G/N\}$$

given by

$$J \mapsto J/N$$

is a bijection.

Proof. Let $A := \{J : N \leq J \leq G\}$ and $B := \{X : X \leq G/N\}$. Clearly $J/N \leq G/N$.
Suppose $J_{1,2} \in A$ and $f(J_1) = f(J_2)$, and let $x \in J_1$. Then

$$xN \in f(J_1) = f(J_2) = J_2/N,$$

so $xN = yN$ for some $y \in J_2$. Since $x \in xN$, $x = yn \in J_2$ for some $n \in N$. It follows that $J_1 \subseteq J_2$, and symmetrically $J_2 \subseteq J_1$. Hence f is injective.
Let $X \in B$ and set $Y = \{y \in G : yN \in X\}$. One can see that $Y \leq G$ since $y_{1,2}N \in X \Rightarrow (y_1N)(y_2N)^{-1} \in X \Rightarrow y_1y_2^{-1}N \in X$, so $y_1y_2^{-1} \in Y$ by definition, hence $Y \leq G$. Since $N \leq Y$ ($nN = N = 1_{G/N} \in X\ \forall n \in N$) one has $y \in A$. Since $f(Y) = X$, f is surjective. $\square$

2 Group action

3 Sylow's theorems

4 Classifying groups of small order

5 Soluble group