Abstract Algebra I

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 341

Subsection 1

Definitions and Examples

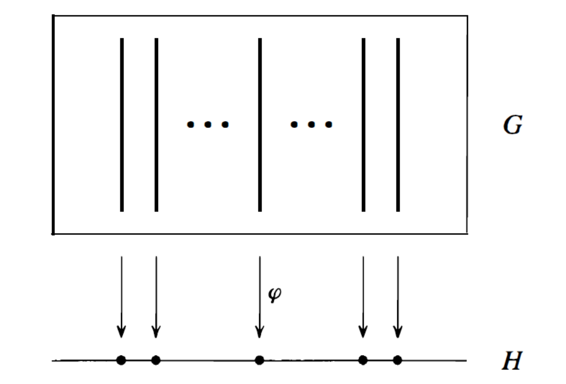
Subgroups and Quotients

- Taking a subgroup of a group results in a "smaller" group.
- Another way to study "smaller" groups is to take quotients.
- The structure of the group G is reflected in the structure of the quotient groups and the subgroups of G:
  - The lattice of subgroups for a quotient of G is reflected at the "top" of the lattice for G;
  - The lattice for a subgroup of G occurs naturally at the "bottom."

  Information about the group G itself can be obtained by combining this information on quotients and subgroups.
- The study of the quotient groups of G is essentially equivalent to the study of the homomorphisms of G, i.e., the maps of the group G to another group which respect the group structures.

Illustration of Homomorphisms and Fibers

- If φ is a homomorphism from G to a group H, the fibers of φ are the sets of elements of G projecting to single elements of H:



Multiplying Fibers

- Consider a homomorphism $\varphi : G \to H$.

  The group operation in H provides a natural multiplication of the fibers lying above two points making the set of fibers into a group:

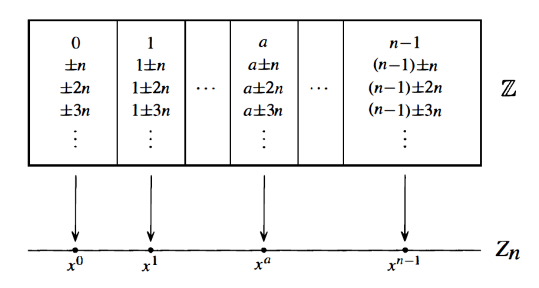
  If X_a is the fiber above a and X_b is the fiber above b, then the product of X_a with X_b is defined to be the fiber X_{ab} above the product ab, i.e.,
  $$X_a X_b = X_{ab}.$$

  - This multiplication is associative since multiplication is associative in H:
  $$(X_a X_b) X_c = X_{ab} X_c = X_{(ab)c} = X_{a(bc)} = X_a X_{bc} = X_a (X_b X_c).$$
  - The identity is the fiber over the identity of H.
  - The inverse of the fiber over a is the fiber over a^{-1}.

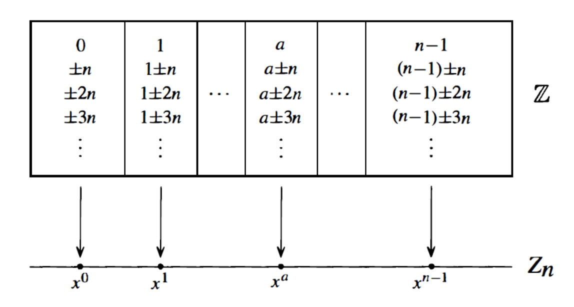
  The fibers of G, with this group structure, form quotient group of G.
- By construction the quotient group with this multiplication is naturally isomorphic to the image of G under the homomorphism φ.

An Example of a Quotient Group

- Let $G = \mathbb{Z}$ and let $H = Z_n = \langle x \rangle$ be the cyclic group of order n. Define $\varphi : \mathbb{Z} \to Z_n$ by $\varphi(a) = x^a$.
  - For $a, b \in \mathbb{Z}$, $\varphi(a+b) = x^{a+b} = x^a x^b = \varphi(a)\varphi(b)$. Hence φ is a homomorphism.
  - φ is surjective.
  - The fiber of φ over x^a is $\varphi^{-1}(x^a) = \{m \in \mathbb{Z} : x^m = x^a\} = \{m \in \mathbb{Z} : x^{m-a} = 1\} = \{m \in \mathbb{Z} : n \text{ divides } m - a\} = \{m \in \mathbb{Z} : m \equiv a \pmod{n}\} = \overline{a}$, i.e., the fibers of φ are precisely the residue classes modulo n:



Example of a Quotient Group (Cont'd)



- The multiplication in Z_n is just $x^a x^b = x^{a+b}$. The corresponding fibers are $\overline{a}, \overline{b}$ and $\overline{a+b}$. The corresponding group operation for the fibers is $\overline{a} \cdot \overline{b} = \overline{a+b}$, which is just the group $\mathbb{Z}/n\mathbb{Z}$ under addition. It is a group isomorphic to the image of φ, which is all of Z_n.
- The identity of this group, the fiber above the identity in Z_n, consists of all the multiples of n in $\mathbb{Z}$, namely $n\mathbb{Z}$, a subgroup of $\mathbb{Z}$.
- The remaining fibers are just translates $a + n\mathbb{Z}$ of this subgroup.

Kernels and First Properties of Homomorphisms

Definition (The Kernel of a Homomorphism)

If φ is a homomorphism $\varphi : G \to H$, the **kernel** of φ is the set

$$\ker\varphi = \{g \in G : \varphi(g) = 1\}.$$

Proposition (Properties of Homomorphisms)

Let G and H be groups and let $\varphi : G \to H$ be a homomorphism.

(1) $\varphi(1_G) = 1_H$, where 1_G and 1_H are the identities of G and H.

(2) $\varphi(g^{-1}) = \varphi(g)^{-1}$, for all $g \in G$.

(3) $\varphi(g^n) = \varphi(g)^n$, for all $n \in \mathbb{Z}$.

(4) $\ker\varphi$ is a subgroup of G.

(5) $\text{im}(\varphi)$, the image of G under φ, is a subgroup of H.

(1) We have $\varphi(1_G)\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)$. By the cancelation laws, we get $\varphi(1_G) = 1_H$.

Proof of Properties (2) and (3)

(2) $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1_G)$ and, by Part (1), $\varphi(1_G) = 1_H$. Hence, $\varphi(g)\varphi(g^{-1}) = 1_H$. Multiplying both sides on the left by $\varphi(g)^{-1}$ gives $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(3) For $n = 0$, we get $\phi(g^0) = \phi(1_G) \stackrel{(1)}{=} 1_H = \phi(g)^0$.

We show the result for $n \in \mathbb{Z}^+$ by induction on n.

- For $n = 1$, $\phi(g^1) = \phi(g) = \phi(g)^1$.
- Assume $\phi(g^n) = \phi(g)^n$.
- Now we have $\phi(g^{n+1}) = \phi(g^n g) = \phi(g^n)\phi(g) = \phi(g)^n\phi(g) = \phi(g)^{n+1}$.

Finally, for $n < 0$, we get

$$\phi(g^n) = \phi((g^{-n})^{-1}) \stackrel{(2)}{=} \phi(g^{-n})^{-1} \stackrel{-n \geq 0}{=} (\phi(g)^{-n})^{-1} = \phi(g)^n.$$

Proof of Properties (4) and (5)

(4) Since $1_G \in \ker\varphi$, the kernel of φ is not empty.
Let $x, y \in \ker\varphi$, i.e., $\varphi(x) = \varphi(y) = 1_H$. Then $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = 1_H 1_H^{-1} = 1_H$. This shows, $xy^{-1} \in \ker\varphi$. By the subgroup criterion, $\ker\varphi \leq G$.

(5) Since $\varphi(1_G) = 1_H$, the identity of H lies in the image of φ. So $\text{im}(\varphi)$ is nonempty.
Suppose x and y are in $\text{im}(\varphi)$, say $x = \varphi(a)$, $y = \varphi(b)$. Then $y^{-1} = \varphi(b^{-1})$ by Part (2). So $xy^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$. Hence, also xy^{-1} is in the image of φ. We conclude $\text{im}(\varphi)$ is a subgroup of H by the subgroup criterion.

Quotient or Factor Groups

Definition (Quotient or Factor Group)

Let $\varphi : G \to H$ be a homomorphism with kernel K. The **quotient group** or **factor group**, G/K (read G **modulo** K or, simply, G **mod** K), is the group whose elements are the fibers of φ with group operation defined by:

> If X is the fiber above a and Y is the fiber above b then the product of X with Y is defined to be the fiber above the product ab.

- The notation emphasizes the fact that the kernel K is a single element in the group G/K and, as in the case of $\mathbb{Z}/n\mathbb{Z}$, the other elements of G/K are just the "translates" of the kernel K.
- Thus, G/K is obtained by collapsing or "dividing out" by K (by equivalence modulo K), explaining the name "quotient" group.

The Fibers in G/K

Proposition

Let $\varphi : G \to H$ be a homomorphism of groups with kernel K. Let $X \in G/K$ be the fiber above a, i.e., $X = \varphi^{-1}(a)$. Then:

(1) For any $u \in X$, $X = \{uk : k \in K\}$;

(2) For any $u \in X$, $X = \{ku : k \in K\}$.

- We prove Part (1) (Part (2) can be proven similarly): Let $u \in X$. By definition of X, $\varphi(u) = a$. Let $uK = \{uk : k \in K\}$.
  - We first prove $uK \subseteq X$: For any $k \in K$, $\varphi(uk) = \varphi(u)\varphi(k) = a1 = a$. So $uk \in X$. This proves $uK \subseteq X$.
  - We now establish $X \subseteq uK$. Suppose $g \in X$ and let $k = u^{-1}g$. Then $\varphi(k) = \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g) = a^{-1}a = 1$. Thus $k \in \ker\varphi$. Since $k = u^{-1}g$, $g = uk \in uK$. Therefore, $X \subseteq uK$.

This proves Part (1).

Left and Right Cosets

Definition (Left and Right Coset)

For any $N \leq G$ and any $g \in G$, let

$$gN = \{gn : n \in N\} \quad \text{and} \quad Ng = \{ng : n \in N\},$$

called respectively a **left coset** and a **right coset** of N in G. Any element of a coset is called a **representative** for the coset.

- We saw that, if N is the kernel of a homomorphism and g_1 is any representative for the coset gN then $g_1 N = gN$ (and, if $g_1 \in Ng$, then $Ng_1 = Ng$).
  This fact provides an explanation for the terminology of a representative.
- If G is an additive group, we write $g + N$ and $N + g$ for the left and right cosets of N in G with representative g, respectively.

Multiplication of Cosets

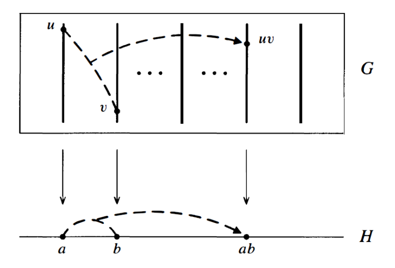
Theorem

Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set whose elements are the left cosets of K in G, with operation defined by $uK \circ vK = (uv)K$, forms a group G/K. In particular, this operation is well defined in the sense that if u_1 is any element in uK and v_1 is any element in vK, then $u_1 v_1 \in uvK$, i.e., $u_1 v_1 K = uvK$, so that the multiplication does not depend on the choice of representatives for the cosets. The same statement is true with "right coset" in place of "left coset".

- Let $X, Y \in G/K$ and let $Z = XY$ in G/K. Thus, X, Y and Z are (left) cosets of K. By assumption, K is the kernel of some homomorphism $\varphi : G \to H$, so $X = \varphi^{-1}(a)$ and $Y = \varphi^{-1}(b)$, for some $a, b \in H$. By definition of the operation in G/K, $Z = \varphi^{-1}(ab)$. Let u and v be arbitrary representatives of X, Y, respectively. Then $\varphi(u) = a$, $\varphi(v) = b$ and $X = uK$, $Y = vK$. We must show $uv \in Z$.

Multiplication of Cosets (Cont'd)

- Using the diagram we must show that $uv \in Z = \varphi^{-1}(ab)$.



We have $uv \in Z$ iff $uv \in \varphi^{-1}(ab)$ iff $\varphi(uv) = ab$ iff $\varphi(u)\varphi(v) = ab$. Since $\varphi(u) = a$ and $\varphi(v) = b$, the last equality holds, showing that $uv \in Z$, whence Z is the (left) coset uvK.

The last statement in the theorem now follows, since, by the preceding proposition, $uK = Ku$ and $vK = Kv$, for all u and v in G.

- The coset uK containing a representative u is denoted $\overline{u}$. With this notation , the quotient group G/K is denoted $\overline{G}$ and the product of elements $\overline{u}$ and $\overline{v}$ is the coset containing uv, i.e., $\overline{uv}$. This notation also emphasizes the fact that the cosets uK in G/K are elements $\overline{u}$ in G/K.

The Homomorphism from $\mathbb{Z}$ to Z_n

- Recall the homomorphism φ from $\mathbb{Z}$ to Z_n that has fibers the left (and also the right) cosets $a + n\mathbb{Z}$ of the kernel $n\mathbb{Z}$.
  The theorem shows that these cosets form the group $\mathbb{Z}/n\mathbb{Z}$ under addition of representatives.
  The group is naturally isomorphic to its image under φ, so we recover the isomorphism $\mathbb{Z}/n\mathbb{Z} \cong Z_n$.

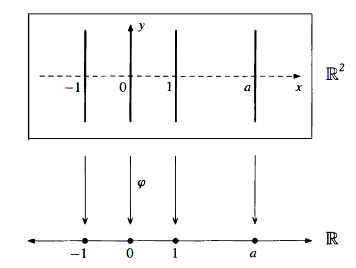
Isomorphisms and Trivial Homomorphisms

- If $\varphi : G \to H$ is an isomorphism, then $K = 1$. The fibers of φ are the singleton subsets of G. So $G/1 \cong G$.
- Let G be any group, let $H = 1$ be the group of order 1 and define $\varphi : G \to H$ by $\varphi(g) = 1$, for all $g \in G$. It is immediate that φ is a homomorphism. This map is called the **trivial homomorphism**. In this case $\ker\varphi = G$. Thus, G/G is a group with the single element G, i.e., $G/G \cong Z_1 = \{1\}$.

Projection Onto the x-Axis

- Let $G = \mathbb{R}^2$, with operation vector addition, and $H = \mathbb{R}$, with operation addition. Define $\varphi : \mathbb{R}^2 \to \mathbb{R}$ by $\varphi((x, y)) = x$. Thus, φ is projection onto the x-axis. We show φ is a homomorphism:
  $\varphi((x_1, y_1) + (x_2, y_2)) = \varphi((x_1 + x_2, y_1 + y_2)) = x_1 + x_2 =$
  $\varphi((x_1, y_1)) + \varphi((x_2, y_2))$.
  Now $\ker\varphi = \{(x, y) : \varphi((x, y)) = 0\} = \{(x, y) : x = 0\} =$ the y-axis.
  Note that $\ker\varphi$ is a subgroup of $\mathbb{R}^2$.

  The fiber of φ over $a \in \mathbb{R}$ is the translate of the y-axis by a, i.e., the line $x = a$. This is also the left (and the right) coset of the kernel with representative $(a, 0)$: $\overline{(a, 0)} = (a, 0) + y$-axis.



The Quaternion Group and the Klein 4-Group

- An example with G non-abelian: Let $G = Q_8$ and let $H = V_4$ be the Klein 4-group. Define $\varphi : Q_8 \to V_4$ by

$$\varphi(\pm 1) = 1,\ \varphi(\pm i) = a,\ \varphi(\pm j) = b,\ \varphi(\pm k) = c.$$

  The check that φ is a homomorphism involves checking that $\varphi(xy) = \varphi(x)\varphi(y)$, for all $x, y \in Q_8$.
  It is clear that φ is surjective.
  $\ker\varphi = \{\pm 1\}$.
  The fibers of φ are the sets $E = \{\pm 1\}$, $A = \{\pm i\}$, $B = \{\pm j\}$ and $C = \{\pm k\}$, which are collapsed to $1, a, b$ and c, respectively in $Q_8/\langle \pm 1\rangle$
  These are the left (and also the right) cosets of $\ker\varphi$.

Coset Partition of a Group

- The cosets of an arbitrary subgroup of G **partition** G, i.e., their union is all of G and distinct cosets have empty intersection.

Proposition

Let N be any subgroup of the group G. The set of left cosets of N in G form a partition of G. Furthermore, for all $u, v \in G$, $uN = vN$ if and only if $v^{-1}u \in N$. In particular, $uN = vN$ if and only if u and v are representatives of the same coset.

- Since N is a subgroup of G, $1 \in N$. Thus, $g = g \cdot 1 \in gN$, for all $g \in G$, i.e., $G = \bigcup_{g \in G} gN$. To show that distinct left cosets have empty intersection, suppose $uN \cap vN \neq \emptyset$. We show $uN = vN$. Let $x \in uN \cap vN$. Write $x = un = vm$, for some $n, m \in N$. Multiplying on the right by n^{-1}, $u = vmn^{-1} = vm_1$, where $m_1 = mn^{-1} \in N$. Now, for any element ut of uN $(t \in N)$, $ut = (vm_1)t = v(m_1t) \in vN$. This proves $uN \subseteq vN$. By interchanging the roles of u and v one obtains similarly that $vN \subseteq uN$.

Coset Partition of a Group (Cont'd)

- We showed that two cosets with nonempty intersection coincide. By the first part,

$$\begin{array}{rll} uN = vN & \text{if and only if} & u \in vN \\ & \text{if and only if} & u = vn, \text{ for some } n \in N, \\ & \text{if and only if} & v^{-1}u \in N. \end{array}$$

  Finally, $v \in uN$ is equivalent to saying v is a representative for uN. Hence $uN = vN$ if and only if u and v are representatives for the same coset, the coset $uN = vN$.

The Group of Cosets

Proposition

Let G be a group and let N be a subgroup of G.

(1) The operation on the set of left cosets of N in G described by $uN \cdot vN = (uv)N$ is well defined if and only if $gng^{-1} \in N$, for all $g \in G$ and all $n \in N$.

(2) If the above operation is well defined, then it makes the set of left cosets of N in G into a group: The identity of this group is the coset $1N$ and the inverse of gN is the coset $g^{-1}N$, i.e., $(gN)^{-1} = g^{-1}N$.

(1) Assume, first, that this operation is well defined, that is, for all $u, v \in G$, if $u, u_1 \in uN$ and $v, v_1 \in vN$, then $uvN = u_1v_1N$. Let g be an arbitrary element of G and let n be an arbitrary element of N. Let $u = 1$, $u_1 = n$ and $v = v_1 = g^{-1}$. Apply the assumption to get $1g^{-1}N = ng^{-1}N$, i.e., $g^{-1}N = ng^{-1}N$. Since $1 \in N$, $ng^{-1} \cdot 1 \in ng^{-1}N$. Thus $ng^{-1} \in g^{-1}N$, hence $ng^{-1} = g^{-1}n_1$, for some $n_1 \in N$. Multiplying on the left by g, $gng^{-1} = n_1 \in N$.

The Group of Cosets (Cont'd)

- Conversely, assume $gng^{-1} \in N$, for all $g \in G$ and all $n \in N$. Let $u, u_1 \in uN$ and $v, v_1 \in vN$. We may write $u_1 = un$ and $v_1 = vm$, for some $n, m \in N$. We must prove that $u_1 v_1 \in uvN$:
  $u_1 v_1 = (un)(vm) = u(vv^{-1})nvm = (uv)(v^{-1}nv)m = (uv)(n_1 m)$, where $n_1 = v^{-1}nv = (v^{-1})n(v^{-1})^{-1}$ is an element of N by assumption. Since N is closed under products, $n_1 m \in N$. Thus, $u_1 v_1 = (uv)n_2$, for some $n_2 \in N$. Thus, the left cosets uvN and $u_1 v_1 N$ contain the common element $u_1 v_1$. By the preceding proposition they are equal, whence the operation is well defined.

(2) If the operation on cosets is well defined the group axioms are easy to check and are induced by their validity in G. E.g., the associative law holds because for all $u, v, w \in G$, $(uN)(vNwN) = uN(vwN) = u(vw)N = (uv)wN = (uvN)(wN) = (uNvN)(wN)$, since $u(vw) = (uv)w$ in G. By the definition of the multiplication, the identity in G/N is the coset $1N$ and the inverse of gN is $g^{-1}N$.

Conjugates and Normal Subgroups

Definition (Conjugate and Normal Subgroup)

Let G be a group and N a subgroup of G.

- The element gng^{-1} is called the **conjugate** of $n \in N$ by $g \in G$.
- The set $gNg^{-1} = \{gng^{-1} : n \in N\}$ is called the **conjugate** of N by $g \in G$.
- The element $g \in G$ is said to **normalize** N if $gNg^{-1} = N$.
- N is called a **normal subgroup** of G if every element of G normalizes N, i.e., if $gNg^{-1} = N$, for all $g \in G$. In this case, we write $N \trianglelefteq G$.

- Note that the structure of G is reflected in the structure of the quotient G/N when N is a normal subgroup.
  - E.g., the associativity of the multiplication in G/N is induced from the associativity in G;
  - Inverses in G/N are induced from inverses in G.

Criteria for Normality

Theorem (Criteria for Normality)

Let N be a subgroup of the group G. The following are equivalent:

(1) $N \trianglelefteq G$;

(2) $N_G(N) = G$ (where $N_G(N)$ is the normalizer in G of N);

(3) $gN = Ng$, for all $g \in G$;

(4) The operation on the left cosets of N in G described in the preceding proposition makes the set of left cosets into a group;

(5) $gNg^{-1} \in N$, for all $g \in G$.

- We have seen almost all equivalences already.

Remarks on Computations for Proving Normality

- To determine whether a given subgroup N is normal in a group G, we would like to avoid as much as possible the computation of all the conjugates gng^{-1} for $n \in N$ and $g \in G$.
  - The elements of N itself normalize N since N is a subgroup.
  - If one has a set of generators for N, it suffices to check that all conjugates of these generators lie in N. This holds because:
    - the conjugate of a product is the product of the conjugates;
    - the conjugate of the inverse is the inverse of the conjugate.
  - If generators for G are known, then it suffices to check that these generators for G normalize N.
  - Even more convenient, if generators for both N and G are known, this reduces the calculations to a small number of conjugations to check.
  - If N is a finite group, then it suffices to check that the conjugates of a set of generators for N by a set of generators for G are in N.
  - Verifying $N_G(N) = G$ can, sometimes, be accomplished without computing all possible conjugates gng^{-1}.

Normal Subgroups as Kernels of Homomorphisms

- Normal subgroups are the same as the kernels of homomorphisms:

Proposition

A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.

- If N is the kernel of the homomorphism φ, then we have seen that the left cosets of N are the same as the right cosets of N (and both are the fibers of the map φ). By the normality criterion, N is then a normal subgroup.
  Conversely, if $N \trianglelefteq G$, let $H = G/N$ and define $\pi : G \to G/N$ by $\pi(g) = gN$, for all $g \in G$. By definition of the operation in G/N,
  $$\pi(g_1g_2) = (g_1g_2)N = g_1Ng_2N = \pi(g_1)\pi(g_2).$$
  This proves π is a homomorphism. Now $\ker\pi = \{g \in G : \pi(g) = 1N\} = \{g \in G : gN = 1N\} = \{g \in G : g \in N\} = N$. Thus N is the kernel of the homomorphism π.

Natural Projection Homomorphisms

- The homomorphism π of the preceding proof is given a special name:

Definition (Natural Projection)

Let $N \trianglelefteq G$. The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called the **natural projection (homomorphism)** of G onto G/N.
If $\overline{H} \leq G/N$ is a subgroup of G/N, the **complete preimage** of $\overline{H}$ in G is the preimage of $\overline{H}$ under the natural projection homomorphism.

- The complete preimage of a subgroup of G/N is a subgroup of G which contains the subgroup N, since N consists of the elements which map to the identity $\overline{1} \in \overline{H}$.
- We will see that there is a natural correspondence between the subgroups of G containing N and the subgroups of the quotient G/N.

Normal Subgroups and Normalizers

- One of the criteria for normality, i.e., for a subgroup being the kernel of a homomorphism, is

$$N \trianglelefteq G \quad \text{iff} \quad N_G(N) = G.$$

- Thus, the normalizer of a subgroup N of G is, in a sense, a measure of "how close" N is to being a normal subgroup.

  This explains the choice of name for the subgroup.
- It is important to keep in mind that the property of being normal is an **embedding property**, i.e., it depends on the relation of N to G, not on the internal structure of N itself.

  In particular, this means that the same group N may be a normal subgroup of G but not a normal subgroup of a larger group containing G.

The Quotient Groups of Cyclic Groups

- For a group G, the subgroups 1 and G are always normal in G. $G/1 \cong G$ and $G/G \cong 1$.
- If G is an abelian group, any subgroup N of G is normal because, for all $g \in G$ and all $n \in N$, $gng^{-1} = gg^{-1}n = n \in N$.

  It is important that G be abelian, not just that N be abelian.

  The structure of G/N may vary for different subgroups N of G.

  - If $G = \mathbb{Z}$, then every subgroup N of G is cyclic: $N = \langle n \rangle = \langle -n \rangle = n\mathbb{Z}$, for some $n \in \mathbb{Z}$. Moreover, $G/N = \mathbb{Z}/n\mathbb{Z}$ is a cyclic group with generator $\overline{1} = 1 + n\mathbb{Z}$ (1 is a generator for G).
  - Suppose $G = Z_k$ is the cyclic group of order k. Let x be a generator of G and let $N \leq G$. We know that $N = \langle x^d \rangle$, where d is the smallest power of x which lies in N. Now $G/N = \{gN : g \in G\} = \{x^a N : a \in \mathbb{Z}\}$ and, since $x^a N = (xN)^a$, it follows that $G/N = \langle xN \rangle$, i.e., G/N is cyclic with xN as a generator.
    - The order of xN in G/N equals d and $d = \frac{|G|}{|N|}$.

The Klein 4-Group as a Quotient of the Quaternion Group

- If $N \leq Z(G)$, then $N \trianglelefteq G$ because, for all $g \in G$ and all $n \in N$, $gng^{-1} = n \in N$. In particular, $Z(G) \trianglelefteq G$.
- The subgroup $\langle -1 \rangle$ of Q_8 was previously seen to be the kernel of a homomorphism. Since $\langle -1 \rangle = Z(Q_8)$, normality of this subgroup is obtained in a different way.
- We also saw that $Q_8/\langle -1 \rangle \cong V_4$. This can also be seen as follows:

  Let $G = D_8$ and $Z = \langle r^2 \rangle = Z(D_8)$. Since $Z = \{1, r^2\}$, each coset gZ consists of the two element set $\{g, gr^2\}$. Since these cosets partition the 8 elements of D_8 into pairs, there must be 4 (disjoint) left cosets of Z in D_8:

$$\overline{1} = 1Z, \quad \overline{r} = rZ, \quad \overline{s} = sZ, \quad \overline{rs} = rsZ.$$

  By the classification of groups of order 4, we know that $D_8/Z(D_8) \cong Z_4$ or V_4. To determine which of these two is correct, observe that $(\overline{r})^2 = r^2 Z = 1Z = \overline{1}$, $(\overline{s})^2 = s^2 Z = 1Z = \overline{1}$ and $(\overline{rs})^2 = (rs)^2 Z = 1Z = \overline{1}$. So every nonidentity element in D_8/Z has order 2. In particular there is no element of order 4 in the quotient. Hence D_8/Z is not cyclic. Therefore, $D_8/Z(D_8) \cong V_4$.

Subsection 2

More on Cosets and Lagrange's Theorem

Lagrange's Theorem

Theorem (Lagrange's Theorem)

If G is a finite group and H is a subgroup of G, then the order of H divides the order of G, i.e., $|H| \mid |G|$, and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.

- Let $|H| = n$ and let the number of left cosets of H in G equal k. We know that the set of left cosets of H in G partition G. By definition of a left coset, the map: $H \to gH$ defined by $h \mapsto gh$ is a surjection from H to the left coset gH. The left cancelation law implies this map is injective, since $gh_1 = gh_2$ implies $h_1 = h_2$. This proves that H and gH have the same order: $|gH| = |H| = n$. Since G is partitioned into k disjoint subsets each of which has cardinality n, $|G| = kn$. Thus, $k = \frac{|G|}{n} = \frac{|G|}{|H|}$.

Index of a Subgroup in a Group

Definition (Index of a Subgroup in a Group)

If G is a group (possibly infinite) and $H \leq G$, the number of left cosets of H in G is called the **index** of H in G and is denoted by $|G : H|$.

- In the case of finite groups the index of H in G is $\frac{|G|}{|H|}$.
- For G an infinite group the quotient $\frac{|G|}{|H|}$ does not make sense. Infinite groups may have subgroups of finite or infinite index.

  Example: Consider the additive group $\mathbb{Z}$:
  - $\{0\}$ is of infinite index in $\mathbb{Z}$.
  - $\langle n \rangle$ is of index n in $\mathbb{Z}$, for every $n > 0$.

Consequences of Lagrange's Theorem

Corollary

If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular, $x^{|G|} = 1$, for all x in G.

- We have seen that $|x| = |\langle x \rangle|$. The first part of the corollary follows from Lagrange's Theorem applied to $H = \langle x \rangle$. For the second statement, since $|G|$ is a multiple of the order of x, $|G| = k|x|$, we get $x^{|G|} = x^{k|x|} = (x^{|x|})^k = 1^k = 1$.

Corollary

If G is a group of prime order p, then G is cyclic. Hence $G \cong Z_p$.

- Let $x \in G$, $x \neq 1$. Thus, $|\langle x \rangle| > 1$ and $|\langle x \rangle| \mid |G|$. Since $|G|$ is prime we must have $|\langle x \rangle| = |G|$. Hence $G = \langle x \rangle$ is cyclic. Every cyclic group of order p is isomorphic to Z_p.

The Symmetric Group S_3

Claim: Let $G = S_3$ and $H = \langle(1\ 2\ 3)\rangle \leq S_3$. Then $H \trianglelefteq S_3$.

We have $H \leq N_G(H) \leq G$.
By Lagrange's Theorem, the order of H divides the order of $N_G(H)$ and the order of $N_G(H)$ divides the order of G. Since G has order 6 and H has order 3, the only possibilities for $N_G(H)$ are H or G.
A direct computation gives

$$(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2) = (1\ 2\ 3)^{-1}.$$

Since $(1\ 2) = (1\ 2)^{-1}$, $(1\ 2)$ conjugates a generator of H to another generator of H. This suffices to prove that $(1\ 2) \in N_G(H)$. Thus $N_G(H) \neq H$. So $N_G(H) = G$, i.e., $H \trianglelefteq S_3$, as claimed.

A Group with a Subgroup of Index 2

Claim: Let G be any group containing a subgroup H of index 2. Then $H \trianglelefteq G$.

Let $g \in G - H$. By hypothesis, the two left cosets of H in G are $1H$ and gH. Since $1H = H$ and the cosets partition G, we must have $gH = G - H$. The two right cosets of H in G are $H1$ and Hg. Since $H1 = H$, we again must have $Hg = G - H$. Combining these gives $gH = Hg$, so every left coset of H in G is a right coset. By the normality criterion, $H \trianglelefteq G$. By definition of index, $|G/H| = 2$, so that $G/H \cong Z_2$.

- This result proves the following:
  - $\langle i \rangle = \{1, i, -1, -i\}, \langle j \rangle = \{1, j, -1, -j\}$ and $\langle k \rangle = \{1, k, -1, -k\}$ are normal subgroups of Q_8;
  - $\langle s, r^2 \rangle = \{1, r^2, s, sr^2\}, \langle r \rangle = \{1, r, r^2, r^3\}$ and $\langle sr, r^2 \rangle = \{1, r^2, sr, sr^3\}$ are normal subgroups of D_8.

Non-Transitivity of $\trianglelefteq$

Claim: The property "is a normal subgroup of" is not transitive.

- We have

  $$\langle s \rangle = \{1, s\},\ \langle s, r^2 \rangle = \{1, r^2, s, sr^2\},\ D_8 = \{s^i r^j : i = 0, 1, 0 \leq j \leq 3\}.$$

  Therefore $\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$ (each subgroup is of index 2 in the next).
- On the other hand, $\langle s \rangle$ is not normal in D_8 because

  $$rsr^{-1} = sr^2 \notin \langle s \rangle.$$

Abelian Groups and Simple Groups

- In abelian groups every subgroup is normal.

  If $H \leq G$ and G is abelian, then, for all $g \in G$,

$$\begin{array}{rcl} g^{-1}Hg & = & \{ghg^{-1} : h \in H\} \\ & = & \{gg^{-1}h : h \in H\} \\ & = & \{h : h \in H\} \\ & = & H. \end{array}$$

- This is not the case in non-abelian groups (in some sense, Q_8 is the unique exception to this).
- There exist groups G in which the only normal subgroups are the trivial ones: 1 and G.

  Such groups are called **simple groups**.

A Non Normal Subgroup of S_3

- Let $H = \langle (1\ 2) \rangle \leq S_3$. Since H is of prime index 3 in S_3, by Lagrange's Theorem $N_{S_3}(H) = H$ or S_3. But $(1\ 3)(1\ 2)(1\ 3)^{-1} = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin H$. So $N_{S_3}(H) \neq S_3$. Thus, H is not a normal subgroup of S_3.

  One can also see this by considering the left and right cosets of H.
  - $(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$;
  - $H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$.

  Since the left coset $(1\ 3)H$ is the unique left coset of H containing $(1\ 3)$, the right coset $H(1\ 3)$ cannot be a left coset.
- The "group operation" on the left cosets of H in S_3 defined by multiplying representatives is not even well defined.
  - For $1H$ and $(1\ 3)H$, 1 and $(1\ 2)$ are both in $1H$;
  - On the other hand, $1 \cdot (1\ 3) = (1\ 3)$ and $(1\ 2) \cdot (1\ 3) = (1\ 3\ 2)$ are not both elements of the same left coset.

Non Normal Subgroups of $S_n, n > 2$

- Let $G = S_n$ for some $n \in \mathbb{Z}^+$ and fix some $i \in \{1, 2, \ldots, n\}$. Let $G_i = \{\sigma \in G : \sigma(i) = i\}$ be the stabilizer of the point i.

  Claim: Let $\tau \in G$, such that $\tau(i) = j$. The left coset τG_i consists of the permutations in S_n which take i to j.

  First note that, if $\sigma \in G_i$, then $\tau\sigma(i) = \tau(i) = j$. Thus, all permutations in τG_i take i to j.

  Suppose, conversely, that $\mu \in G$, such that $\mu(i) = j$. Then, we have $\tau^{-1}\mu(i) = \tau^{-1}(j) = i$. Thus, $\tau^{-1}\mu \in G_i$ and, hence, $\mu \in \tau G_i$. Thus, all permutations taking i to j are in τG_i.

  - Distinct left cosets have empty intersection;
  - The number of distinct left cosets is n, the number of distinct images of the integer i under the action of G. Thus, $|G : G_i| = n$.

Non Normal Subgroups of S_n, $n > 2$ (Cont'd)

- Let $G = S_n$ for some $n \in \mathbb{Z}^+$ and fix some $i \in \{1, 2, \ldots, n\}$. Let $G_i = \{\sigma \in G : \sigma(i) = i\}$ be the stabilizer of the point i.

  Claim: Let $\tau \in G$, such that $k = \tau^{-1}(i)$, i.e., $\tau(k) = i$. The right coset $G_i\tau$ consists of the permutations in S_n which take k to i.

  First note that, if $\sigma \in G_i$, then $\sigma\tau(k) = \sigma(i) = i$. Thus, all permutations in $G_i\tau$ take k to i.

  Suppose, conversely, that $\mu \in G$, such that $\mu(k) = i$. Then, we have $\mu\tau^{-1}(i) = \mu(k) = i$. Thus, $\mu\tau^{-1} \in G_i$ and, hence, $\mu \in G_i\tau$. Thus, all permutations taking k to i are in τG_i.
- If $n > 2$, for some nonidentity element τ, we have $\tau G_i \neq G_i\tau$ since there are certainly permutations which take i to j but do not take k to i. Thus G_i is not a normal subgroup.

Non Normal Subgroups of D_8

Claim: In D_8 the only subgroup of order 2 which is normal is the center $\langle r^2 \rangle$.

First, we show that $\langle r^2 \rangle$ is normal:

$$\begin{array}{rcl} r\{1, r^2\} & = & \{r, r^3\} = \{1, r^2\}r; \\ s\{1, r^2\} & = & \{s, sr^2\} = \{s, r^{-2}s\} = \{s, r^2 s\} = \{1, r^2\}s. \end{array}$$

Next we show that none of the other four subgroups of order 2 is normal:

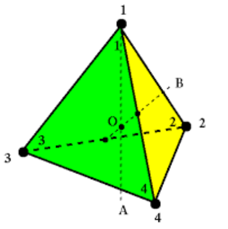
- $\langle s \rangle$: $r\{1, s\} = \{r, rs\} \neq \{r, sr\} = \{1, s\}r$.
- $\langle r^2 s \rangle$: $r\{1, r^2 s\} = \{r, r^3 s\} \neq \{r, rs\} = \{r, r^2 sr\} = \{1, r^2 s\}r$.
- $\langle rs \rangle$: $r\{1, rs\} = \{r, r^2 s\} \neq \{r, s\} = \{r, rsr\} = \{1, rs\}r$.
- $\langle r^3 s \rangle$: $r\{1, r^3 s\} = \{r, s\} \neq \{r, r^2 s\} = \{1, r^3 s\}r$.

Group of Rigid Motions of the Regular Tetrahdron

Claim: The group G of rigid motions of a regular tetrahedron in $\mathbb{R}^3$ has order 12.

Let θ be a rigid motion of the tetrahedron. If the vertices of a face, read clockwise from outside the figure, are XYZ, then $\theta(X)\theta(Y)\theta(Z)$ are the vertices of the corresponding face, read clockwise from outside the figure, of the moved copy.

- There are 4 possibilities for $\theta(1)$.
- Once $\theta(1)$ is chosen, there are 3 possibilities for $\theta(2)$.
- Once $\theta(1)$ and $\theta(2)$ are chosen, $\theta(3)$ is determined by orientation.
- Finally, there is only one possibility remaining for $\theta(4)$.



Thus there are $3 \cdot 4 = 12$ total possibilities for θ, showing that $|G| = 12$.

Remark on Lagrange's Theorem

- The full converse to Lagrange's Theorem is not true: If G is a finite group and n divides $|G|$, then G need not have a subgroup of order n.

  Example: Let A be the group of symmetries of a regular tetrahedron. We know that $|A| = 12$.

  Claim: A does not have a subgroup of order 6.

  If A had a subgroup H of order 6, H would be of index 2 in A, whence $A/H \cong Z_2$. Since the quotient group has order 2, the square of every element in the quotient is the identity, so, for all $g \in A$, $(gH)^2 = 1H$, i.e., for all $g \in A$, $g^2 \in H$. If g is an element of A of order 3, we obtain $g = (g^2)^2 \in H$, i.e., H must contain all elements of A of order 3. This is a contradiction since $|H| = 6$, but there are 8 rotations of a tetrahedron of order 3.

A Counting Formula

Definition

Let H and K be subgroups of a group and define

$$HK = \{hk : h \in H, k \in K\}.$$

Proposition

If H and K are finite subgroups of a group then $|HK| = \frac{|H||K|}{|H \cap K|}$.

- HK is a union of left cosets of K, namely, $HK = \bigcup_{h \in H} hK$. Since each coset of K has $|K|$ elements, it suffices to find the number of distinct left cosets of the form hK, $h \in H$. But $h_1K = h_2K$ for $h_1, h_2 \in H$ if and only if $h_2^{-1}h_1 \in K$. Thus, $h_1K = h_2K$ iff $h_2^{-1}h_1 \in H \cap K$ iff $h_1(H \cap K) = h_2(H \cap K)$. Thus, the number of distinct cosets of the form hK, for $h \in H$ is the number of distinct cosets $h(H \cap K)$, for $h \in H$. The latter number, by Lagrange's Theorem, equals $\frac{|H|}{|H \cap K|}$. Thus HK consists of $\frac{|H|}{|H \cap K|}$ distinct cosets of K (each of which has $|K|$ elements) which yields the formula.

The Set HK

- There was no assumption that HK be a subgroup.

  Example: If $G = S_3$, $H = \langle (1\ 2) \rangle$ and $K = \langle (2\ 3) \rangle$, then $|H| = |K| = 2$ and $|H \cap K| = 1$. So $|HK| = \frac{|H||K|}{|H \cap K|} = 4$.
  By Lagrange's Theorem HK cannot be a subgroup.
  As a consequence, we must have $S_3 = \langle (1\ 2), (2\ 3) \rangle$.

Criterion for HK to be a Subgroup

Proposition

If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.

($\Leftarrow$): Assume, first, that $HK = KH$ and let $a, b \in HK$. We prove $ab^{-1} \in HK$, which suffices to show that HK is a subgroup, by the subgroup criterion. Let $a = h_1 k_1$ and $b = h_2 k_2$, for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Thus, $b^{-1} = k_2^{-1} h_2^{-1}$. So, $ab^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$. Let $k_3 = k_1 k_2^{-1} \in K$ and $h_3 = h_2^{-1}$. Thus, $ab^{-1} = h_1 k_3 h_3$. Since $HK = KH$, $k_3 h_3 = h_4 k_4$, for some $h_4 \in H$, $k_4 \in K$. Thus, $ab^{-1} = h_1 h_4 k_4$. Since $h_1 h_4 \in H$, $k_4 \in K$, we obtain $ab^{-1} \in HK$.
($\Rightarrow$): Conversely, assume that HK is a subgroup of G. Since $K \leq HK$ and $H \leq HK$, by the closure property of subgroups, $KH \subseteq HK$. To show the reverse containment let $hk \in HK$. Since HK is assumed to be a subgroup, write $hk = a^{-1}$, for some $a \in HK$. If $a = h_1 k_1$, then $hk = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH$, completing the proof.

Remarks on the Criterion

- $HK = KH$ does not imply that the elements of H commute with those of K but rather that every product hk is of the form $k'h'$ (h need not be h' nor k be k') and conversely.

  Example: If $G = D_{2n}$, $H = \langle r \rangle$ and $K = \langle s \rangle$, then $G = HK = KH$ so that HK is a subgroup and $rs = sr^{-1}$ so the elements of H do not commute with the elements of K.

Corollary

If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $K \trianglelefteq G$, then $HK \leq G$, for any $H \leq G$.

- We prove $HK = KH$. Let $h \in H$, $k \in K$. By assumption, $hkh^{-1} \in K$, hence $hk = (hkh^{-1})h \in KH$. This proves $HK \subseteq KH$. Similarly, $kh = h(h^{-1}kh) \in HK$, proving the reverse containment. Now the corollary follows from the preceding proposition.

More on the Product HK

Definition

If A is any subset of $N_G(K)$ (or $C_G(K)$), we shall say A **normalizes** K (**centralizes** K, respectively).

- Using this terminology, the preceding corollary states that HK is a subgroup if H normalizes K.
- In some cases, it is possible to prove that a finite group is a product of two of its subgroups by simply using the order formula.

  Example: Let $G = S_4$, $H = D_8$ and $K = \langle (1\ 2\ 3) \rangle$, where we consider D_8 as a subgroup of S_4 by identifying each symmetry with its permutation on the 4 vertices of a square.

  By Lagrange's Theorem, $H \cap K = 1$.

  The proposition then shows $|HK| = \frac{|H||K|}{|H \cap K|} = 24$. So $HK = S_4$. Since HK is a group, $HK = KH$.

  But note that neither H nor K normalizes the other.

Subsection 3

The Isomorphism Theorems

The First Isomorphism Theorem

Theorem (The First Isomorphism Theorem)

If $\varphi : G \to H$ is a homomorphism of groups, then $\ker\varphi \trianglelefteq G$ and $G/\ker\varphi \cong \varphi(G)$.

- We first show that $\ker\varphi \leq G$.
  Since $\varphi(1_G) = 1_H$, $1_G \in \ker\varphi$. Therefore, $\ker\varphi \neq \emptyset$. Suppose that $x, y \in \ker\varphi$. Thus, $\varphi(x) = \varphi(y) = 1_H$. So we get $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = 1_H 1_H^{-1} = 1_H$. Thus, $xy^{-1} \in \ker\varphi$. By the subgroup criterion, we get that $\ker\varphi \leq G$.
  We show next that $\ker\varphi \trianglelefteq G$. We do this by showing that, for all $g \in G$, $g\ker\varphi g^{-1} = \ker\varphi$.
  Suppose $x \in \ker\varphi$. Then $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)1_H\varphi(g)^{-1} = 1_H$. So $gxg^{-1} \in \ker\varphi$. Thus, $g\ker\varphi g^{-1} \subseteq \ker\varphi$.
  Suppose, conversely, that $x \in \ker\varphi$. Then $g^{-1}xg \in \ker\varphi$. And we have $x = g(g^{-1}xg)g^{-1} \in g\ker\varphi g^{-1}$. So $\ker\varphi \subseteq g\ker\varphi g^{-1}$.

The First Isomorphism Theorem (Cont'd)

- Now define $\psi : G/\text{ker}\varphi \to \varphi(G)$ by setting $\psi(g/\text{ker}\varphi) = \varphi(g)$.
  First, we show ψ is well-defined. Suppose that $g_1/\text{ker}\varphi = g_2/\text{ker}\varphi$. Then $g_2^{-1}g_1 \in \text{ker}\varphi$. Hence $\varphi(g_2^{-1}g_1) = 1_H$, i.e., $\varphi(g_2)^{-1}\varphi(g_1) = 1_H$. We get $\varphi(g_1) = \varphi(g_2)$.
  Next we show that ψ is a homomorphism:

$$\begin{array}{rcl} \psi((g_1/\text{ker}\varphi)(g_2/\text{ker}\varphi)) & = & \psi((g_1g_2)/\text{ker}\varphi) \\ & = & \varphi(g_1g_2) \\ & = & \varphi(g_1)\varphi(g_2) \\ & = & \psi(g_1/\text{ker}\varphi)\psi(g_2/\text{ker}\varphi). \end{array}$$

  ψ is clearly onto $\varphi(G)$.
  We finally show that ψ is one-to-one.
  Suppose $\psi(g_1/\text{ker}\varphi) = \psi(g_2/\text{ker}\varphi)$. Then $\varphi(g_1) = \varphi(g_2)$. Thus, $\varphi(g_2^{-1}g_1) = \varphi(g_2)^{-1}\varphi(g_1) = 1_H$. This shows that $g_2^{-1}g_1 \in \text{ker}\varphi$. Therefore $g_1/\text{ker}\varphi = g_2/\text{ker}\varphi$.

Consequences of the First Isomorphism Theorem

Corollary

Let $\varphi : G \to H$ be a homomorphism of groups.

(1) φ is injective if and only if $\ker\varphi = 1$;

(2) $|G : \ker\varphi| = |\varphi(G)|$.

(1) Suppose φ is injective. Then, if $g \in \ker\varphi$, $\varphi(g) = 1_H = \varphi(1_G)$, whence $g = 1_G$. Thus, $\ker\varphi = 1$.
Conversely, assume $\ker\varphi = 1$ and $\varphi(g_1) = \varphi(g_2)$. Then $\varphi(g_1 g_2^{-1}) = 1_H$. Hence, $g_1 g_2^{-1} = 1_G$ i.e., $g_1 = g_2$. Thus, φ is injective.

(2) $|\varphi(G)| = |G/\ker\varphi| = |G : \ker\varphi|$.

The Second or Diamond Isomorphism Theorem

Theorem (The Second or Diamond Isomorphism Theorem)

Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.

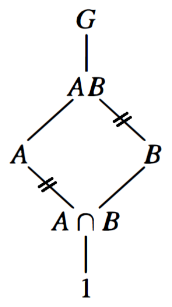
- Since $A \leq N_G(B)$, AB is a subgroup of G. Since $A \leq N_G(B)$, by assumption, and $B \leq N_G(B)$ trivially, it follows that $AB \leq N_G(B)$, i.e., B is a normal subgroup of the subgroup AB.
  Since B is normal in AB, the quotient group AB/B is well defined. Define the map $\varphi : A \to AB/B$ by $\varphi(a) = aB$. Since the group operation in AB/B is well defined, it is easy to see that φ is a homomorphism:
  $$\varphi(a_1 a_2) = (a_1 a_2)B = a_1 B \cdot a_2 B = \varphi(a_1)\varphi(a_2).$$
  Alternatively, the map φ is just the restriction to the subgroup A of the natural projection homomorphism $\pi : AB \to AB/B$, so is also a homomorphism.

Proof of the Second Isomorphism Theorem

- We defined the homomorphism $\varphi : A \to AB/B$ by $\varphi(a) = aB$.

  It is clear from the definition of AB that φ is surjective. The identity in AB/B is the coset $1B$, so the kernel of φ consists of the elements $a \in A$, with $aB = 1B$, which are the elements $a \in B$, i.e., $\ker\varphi = A \cap B$. By the First Isomorphism Theorem, $A \cap B \trianglelefteq A$ and $A/A \cap B \cong AB/B$.

- The reason this theorem is called the Diamond Isomorphism is because of the portion of the lattice of subgroups of G involved. The markings in the lattice lines indicate which quotients are isomorphic.
  - The "quotient" AB/A need not be a group (i.e., A need not be normal in AB).
  - The relation $|AB : A| = |B : A \cap B|$ still holds.



The Third Isomorphism Theorem

- The third Isomorphism Theorem considers the question of taking quotient groups of quotient groups.

Theorem (The Third Isomorphism Theorem)

Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$. If we denote the quotient by H with a bar, this can be written $\overline{G}/\overline{K} \cong G/K$.

- Verify that $K/H \trianglelefteq G/H$. Define $\varphi : G/H \to G/K$ by $(gH) \mapsto gK$.
  - φ is well defined: If $g_1H = g_2H$, then $g_1 = g_2h$, for some $h \in H$. Since $H \leq K$, $h \in K$, whence $g_1K = g_2K$, i.e., $\varphi(g_1H) = \varphi(g_2H)$.
  - Since g may be chosen arbitrarily in G, φ is a surjective homomorphism.
  - Finally, $\ker\varphi = \{gH \in G/H : \varphi(gH) = 1K\} = \{gH \in G/H : gK = 1K\} = \{gH \in G/H : g \in K\} = K/H$.

  By the First Isomorphism Theorem, $(G/H)/(K/H) \cong G/K$.

The Fourth or Lattice Isomorphism Theorem I

- The final isomorphism theorem exhibits a one-to-one correspondence between the subgroups of G containing N and the subgroups of G/N. Thus, the lattice for G/N appears in the lattice for G as the collection of subgroups of G between N and G.

Theorem (The Fourth or Lattice Isomorphism Theorem)

Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N. In particular, every subgroup of G is of the form A/N, for some subgroup A of G containing N (its preimage in G under the natural projection homomorphism from G to G/N). For all $A, B \leq G$ with $N \leq A$ and $N \leq B$, the bijection satisfies:

(1) $A \leq B$ if and only if $\overline{A} \leq \overline{B}$;

(2) if $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$;

(3) $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$;

(4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$;

(5) $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.

The Fourth or Lattice Isomorphism Theorem II

- Denote by $\mathrm{Sub}(G:N)$ the set of subgroups of G containing N and by $\mathrm{Sub}(G/N)$ the set of subgroups of G/N.
  Define $\Psi : \mathrm{Sub}(G:N) \to \mathrm{Sub}(G/N)$, by $\Psi : S \mapsto S/N$.
- This map is well-defined, i.e., if $N \leq S \leq G$, then $S/N \leq G/N$:
  Since $1 \in S$, we get $1/N \in S/N$. Thus, $S/N \neq \emptyset$.
  Next, let $s_1/N, s_2/N \in S/N$. Then $(s_1N)(s_2N)^{-1} = (s_1s_2^{-1})N$ $\in S/N$, since $S \leq G$. By the subgroup criterion, $S/N \leq G/N$.
- We show that Ψ is injective.
  Claim: If $N \leq S \leq G$, then $\pi^{-1}(\pi(S)) = S$, where $\pi : G \to G/N$ is the projection.
  By set theory $S \subseteq \pi^{-1}\pi(S)$. Now, let $a \in \pi^{-1}\pi(S)$. Then $\pi(a) = \pi(s)$, for some $s \in S$. Hence $s^{-1}a \in \ker\pi = N$. So $a = sn$, for some $n \in N$. But $N \leq S$, whence $a = sn \in S$.
  Assume $S/N = S'/N$, where $N \leq S, S' \leq G$. Then $\pi^{-1}\pi(S) = \pi^{-1}\pi(S')$. By the claim, $S = S'$. So Ψ is injective.

The Fourth or Lattice Isomorphism Theorem III

- We Show Ψ is surjective.

  Let $U \leq G/N$. $\pi^{-1}(U) \leq G$. Moreover, $N = \pi^{-1}(\{1\})$, whence $N \leq \pi^{-1}(U)$. Finally, $\pi(\pi^{-1}(U)) = U$. Thus, Ψ is surjective.

(1) We show $A \leq B$ iff $A/N \leq B/N$.

By set theory, if $N \leq A \leq B \leq G$, then $A/N = \pi(A) \leq \pi(B) = B/N$.

Conversely, assume $A/N \leq B/N$. If $a \in A$, then $aN \in A/N \leq B/N$. So $aN = bN$, for some $b \in B$. Hence $a = bn$, for some $n \in N \leq B$. So we get $a \in B$, showing $A \leq B$.

The Fourth or Lattice Isomorphism Theorem IV

(2) We show that, if $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$.
It suffices to show that there is a bijection from the family of all cosets of the form bA, with $b \in B$, to the family of all cosets of the form $c\overline{A}$, with $c \in \overline{B}$. For all $b \in B$, we set $bA \mapsto \overline{bA}$.

- The map is injective.
Suppose that $\overline{b}_1\overline{A} = \overline{b}_2\overline{A}$, for some $b_1, b_2 \in B$. Then, we get $\overline{b}_2^{-1}\overline{b}_1 \in \overline{A}$, i.e., $\overline{b_2^{-1}b_1} \in \overline{A}$. Thus, $b_2^{-1}b_1 = an$, for some $n \in N$. Since $N \leq A$, $b_2^{-1}b_1 \in A$. So $b_1A = b_2A$.
- The map is surjective.
Suppose $\overline{bA} \in \overline{B}/\overline{A}$, for some $\overline{b} \in \overline{B}$. Then $bN = b'N$, for some $b \in B$. So $b'^{-1}b \in N \leq B$. Thus, $b \in B$, whence $bA \in B/A$, and $b/A \mapsto \overline{bA}$.

- Note that for finite G, $|B : A| = |\overline{B} : \overline{A}|$ may be proved as follows:

$$|\overline{B} : \overline{A}| = \frac{|\overline{B}|}{|\overline{A}|} = \frac{|B/N|}{|A/N|} = \frac{\frac{|B|}{|N|}}{\frac{|A|}{|N|}} = \frac{|B|}{|A|} = |B : A|.$$

The Fourth or Lattice Isomorphism Theorem V

(3) We show $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$.

$$\begin{array}{rcl} \overline{\langle A, B\rangle} & = & \{\overline{c_1^{\epsilon_1} c_2^{\epsilon_2} \cdots c_n^{\epsilon_n}} : n \geq 0, c_i \in A \cup B, \epsilon_i = \pm 1\} \\ & = & \{\overline{c}_1^{\epsilon_1} \overline{c}_2^{\epsilon_2} \cdots \overline{c}_n^{\epsilon_n} : n \geq 0, c_i \in A \cup B, \epsilon_i = \pm 1\} \\ & = & \langle \overline{A}, \overline{B}\rangle. \end{array}$$

(4) We show $\overline{A \cap B} = \overline{A} \cap \overline{B}$.

$$\begin{array}{rcl} \overline{A \cap B} & = & \{\overline{c} : c \in A \cap B\} \\ & = & \overline{A} \cap \overline{B}. \end{array}$$

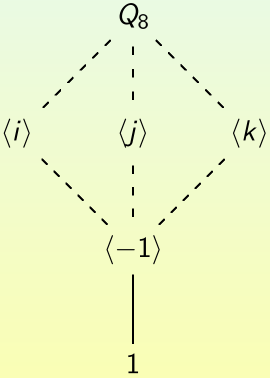
(5) We show $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.

If $A \trianglelefteq G$, then both N and A are normal subgroups of G, with $N \leq A$. By the Third Isomorphism Theorem, $A/N \trianglelefteq G/N$.

Suppose, conversely, that $A/N \trianglelefteq G/N$. Let $a \in A$ and $g \in G$. Then $\overline{gag^{-1}} = \overline{g}\ \overline{a}\ \overline{g}^{-1} \in A/N$. So $gag^{-1} \in A$. This proves that $A \trianglelefteq G$.

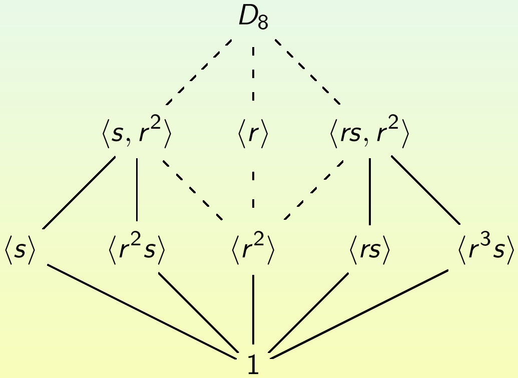
The Quaternion Group

- Consider $G = Q_8$ and let N be the normal subgroup $\langle -1 \rangle$:



The Dihedral Group of Order 8

- Let $G = D_8$ and $N = \langle r^2 \rangle$:

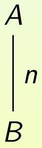


- Note that there are subgroups of G which do not directly correspond to subgroups in the quotient group G/N, namely the subgroups of G which do not contain the normal subgroup N.

Remarks on the Lattices of Subgroups

- The examples of Q_8 and D_8 emphasize the fact that the isomorphism type of a group cannot, in general, be determined from the knowledge of the isomorphism types of G/N and N:

  Indeed $Q_8/\langle -1\rangle \cong D_8/\langle r^2\rangle$ and $\langle -1\rangle \cong \langle r^2\rangle$, but $Q_8 \ncong D_8$.
- We often indicate the index of one subgroup in another in the lattice of subgroups by writing



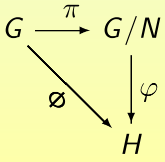
  where the integer $n = |A : B|$.
- The Lattice Isomorphism Theorem shows that indices remain unchanged in quotients of G by normal subgroups of G contained in B, i.e., the portion of the lattice for G corresponding to the lattice of the quotient group has the correct indices for the quotient as well.

Defining Homomorphisms on Quotients

- Sometimes, a homomorphism φ on the quotient group G/N is specified by giving the value of φ on the coset gN in terms of the representative g alone. In that case, one has to show that φ is well defined, i.e., independent of the choice of g.
- This is tantamount to defining a homomorphism Φ on G itself by specifying the value of φ at g. Then independence of g is equivalent to requiring that Φ be trivial on N:

$$\varphi \text{ is well defined on } G/N \text{ if and only if } N \leq \ker\Phi.$$

- In this situation we say the homomorphism Φ **factors through** N and φ is the **induced homomorphism** on G/N:



Subsection 4

Composition Series

Elements of Prime Order in Abelian Groups

Proposition

If G is a finite abelian group and p is a prime dividing $|G|$ then G contains an element of order p.

- The proof proceeds by complete induction on $|G|$: We assume the result is valid for every group whose order is strictly smaller than the order of G and then prove the result valid for G.

  Since $|G| > 1$, there is an element $x \in G$, with $x \neq 1$.
  - If $|G| = p$, then x has order p by Lagrange's Theorem and we are done.
  - We assume, next, that $|G| > p$.

The Case $|G| > p$

- If p divides $|x|$, there exists an n, such that $|x| = pn$. Thus, $|x^n| = p$, and again we have an element of order p.
- Assume p does not divide $|x|$. Let $N = \langle x \rangle$. Since G is abelian, $N \trianglelefteq G$. By Lagrange's Theorem, $|G/N| = \frac{|G|}{|N|}$. Since $N \neq 1$, $|G/N| < |G|$. Since p does not divide $|N|$, we must have $p \mid |G/N|$. By the induction hypothesis, the smaller group G/N contains an element, $\overline{y} = yN$, of order p.
  If $|y| = m$, then
  $$(yN)^m = y^m N = N.$$
  Thus, since $|yN| = p$, we get, by a preceding proposition, $p \mid |y|$. We are now back to the preceding case. The argument used above produces an element of order p.

Simple Groups

Definition (Simple Group)

A (finite or infinite) group G is called **simple** if $|G| > 1$ and the only normal subgroups of G are 1 and G.

- By Lagrange's Theorem, if $|G|$ is a prime, its only subgroups (let alone normal ones) are 1 and G, so G is simple.
- Simple groups, by definition, cannot be "factored" into pieces like N and G/N and, as a result, they play a role analogous to that of the primes in the arithmetic of $\mathbb{Z}$.

Abelian Simple Groups

Claim: Every abelian simple group is isomorphic to Z_p, for some prime p.

Since G is abelian, every subgroup is normal. Since G is simple, $|G| > 1$ and the only subgroups of G are 1 and G. So for some $x \in G$ we have $|x| > 1$ and $\langle x \rangle \leq G$. Hence $\langle x \rangle = G$.

- Suppose x has infinite order. Then $1 \neq \langle x^2 \rangle < \langle x \rangle = G$. This is a contradiction.
- Thus, x, and therefore G, has finite order. Suppose x has composite order n. Then, for some $p > 1$ that divides n, $\langle x^p \rangle$ is a proper non-trivial subgroup of G. Hence G is not simple. We conclude that G is a cyclic group of prime order.

- There are also *non-abelian* simple groups (of both finite and infinite order), the smallest of which has order 60.

Normal Series

- A **normal series** of a group G is a finite sequence of subgroups

$$1 = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_{n-1} \leq G_n = G,$$

such that $G_i \trianglelefteq G_{i+1}$, for all $0 \leq i \leq n-1$.

The **factor groups** of the series are the groups

$$G_1/G_0, G_2/G_1, \ldots, G_n/G_{n-1}.$$

The **length** of the series is the number of strict inclusions or, equivalently, the number of non-trivial factor groups.

Normal Series

Proposition

Suppose G is a finite group and

$$1 = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_{n-1} \leq G_n = G,$$

is a normal series of G. Then the order $|G|$ of G is the product of the orders of the factor groups in the series.

- We have for all $0 \leq i < n$,

$$|G_{i+1}/G_i| = \frac{|G_{i+1}|}{|G_i|} \Rightarrow |G_{i+1}| = |G_{i+1}/G_i| \cdot |G_i|.$$

Therefore, we get

$$\begin{aligned} |G| &= |G_n| = |G_n/G_{n-1}||G_{n-1}| = |G_n/G_{n-1}||G_{n-1}/G_{n-2}||G_{n-2}| \\ &= \cdots = \prod_{i=0}^{n-1} |G_{i+1}/G_i| \cdot |G_0| = \prod_{i=0}^{n-1} |G_{i+1}/G_i|. \end{aligned}$$

Zassenhaus Lemma

Lemma (Zassenhaus Lemma)

Given four subgroups $A \trianglelefteq A'$ and $B \trianglelefteq B'$ of a group G, then $A(A' \cap B) \trianglelefteq A(A' \cap B')$, $B(B' \cap A) \trianglelefteq B(B' \cap A')$, and there is an isomorphism

$$\frac{A(A' \cap B')}{A(A' \cap B)} \cong \frac{B(B' \cap A')}{B(B' \cap A)}.$$

Claim: $(A \cap B') \trianglelefteq (A' \cap B')$, i.e., if $c \in A \cap B'$ and $x \in A' \cap B'$, then $xcx^{-1} \in A \cap B'$.

Since $c \in A$, $x \in A'$ and $A \trianglelefteq A'$, we get $xcx^{-1} \in A$. Since $c, x \in B'$, then $xcx^{-1} \in B'$. Therefore, $(A \cap B') \triangleleft (A' \cap B')$.

Similarly, $(A' \cap B) \trianglelefteq (A' \cap B')$.

Thus, the subgroup $D = (A \cap B')(A' \cap B)$ of G is a normal subgroup of $A' \cap B'$, since it is generated by two normal subgroups.

Zassenhaus Lemma (Cont'd)

Using the symmetry of the claimed isomorphism in A and B, it suffices to show that there is an isomorphism

$$\frac{A(A' \cap B')}{A(A' \cap B)} \to \frac{(A' \cap B')}{D}.$$

Define

$$\varphi : A(A' \cap B') \to (A' \cap B')/D; \quad \varphi : ax \mapsto xD,$$

where $a \in A$ and $x \in A' \cap B'$.

φ is well-defined: If $ax = a'x'$, where $a' \in A$ and $x' \in A' \cap B'$, then

$$a'^{-1}a = x'x^{-1} \in A \cap (A' \cap B') = A \cap B' \leq D.$$

φ is clearly surjective.

Moreover, $\ker\varphi = A(A' \cap B)$.

By the First Isomorphism Theorem, we get the result.

Zassenhaus Lemma and the Diamond Isomorphism

- The Zassenhaus Lemma implies the Diamond Isomorphism Theorem. Suppose that $S, T \leq G$ with $T \trianglelefteq G$. Setting

$$A' = G, \quad A = T, \quad B' = S, \quad B = S \cap T$$

in the Zassenhaus Lemma, we get by the conclusion $\dfrac{A(A' \cap B')}{A(A' \cap B)} \cong \dfrac{B(B' \cap A')}{B(B' \cap A)}$ that

$$\frac{T(G \cap S)}{T(G \cap (S \cap T))} \cong \frac{(S \cap T)(S \cap G)}{(S \cap T)(S \cap T)},$$

i.e.,

$$TS/T \cong S(S \cap T).$$

Composition Series

Definition (Composition Series)

In a group G a sequence of subgroups

$$1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_k = G$$

is called a **composition series** if $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is a simple group, $0 \leq i \leq k-1$. If the above sequence is a composition series, the quotient groups N_{i+1}/N_i are called the **composition factors** of G.

- A composition series is a normal series all of whose nontrivial factors are simple.

  Example: The series

  $$1 \trianglelefteq \langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8 \quad \text{and} \quad 1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_8$$

  are two composition series for D_8. In each series there are 3 composition factors, each of which is isomorphic to (the simple group) Z_2.

Finite Groups have a Composition Series

Proposition

Every finite group G has a composition series.

- If the proposition is false, let G be a finite group of smallest order that does not have a composition series. G cannot be simple, since otherwise $1 \leq G$ is a composition series. Thus, G has a proper normal subgroup N. Assume that N is a maximal normal subgroup, so that G/N is simple. Since $|N| < |G|$, N has a composition series, say

$$1 \leq N_1 \leq \cdots \leq N_{m-1} \leq N_m = N.$$

But, then,

$$1 \leq N_1 \leq N_2 \leq \cdots \leq N_m \leq G$$

is a composition series for G, a contradiction.

Equivalent Series and Refinements

Definition

Two normal series of a group G are **equivalent** if there is a bijection between the sets of nontrivial factor groups of each so that corresponding factor groups are isomorphic.

Definition

A **refinement** of a normal series is a normal series $1 = N_0 \leq N_1 \leq \cdots \leq N_k = G$ having the original series as a subsequence.

- A refinement of a normal series is a new normal series obtained from the original by inserting more subgroups.
- Claim: A composition series admits only trivial refinements, i.e., one can only repeat terms.
  If N_{i+1}/N_i is simple, then it has no proper nontrivial normal subgroups. Hence, there is no intermediate group H, with $N_i < H < N_{i+1}$ and $H \trianglelefteq N_{i+1}$.
  So any refinement of a composition series is equivalent to the original.

The Schreier Refinement Theorem

Theorem (Schreier Refinement Theorem)

Any two normal series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G, \quad 1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_m = G$$

of a group G have equivalent refinements.

- We insert a copy of the second series between each pair of adjacent terms in the first series: for each $i \geq 1$ define $G_{ij} = G_{i-1}(G_i \cap N_j)$, which is a subgroup, since $G_{i-1} \trianglelefteq G_i$. We have $G_{i0} = G_{i-1}(G_i \cap N_0) = G_{i-1}(G_i \cap 1) = G_{i-1}1 = G_{i-1}$. Also $G_{im} = G_{i-1}(G_i \cap N_m) = G_{i-1}(G_i \cap G) = G_{i-1}G_i = G_i$. Therefore the series of G_{ij} is a refinement of the series of G_i:

$$\cdots \leq G_{i-1} = G_{i0} \leq G_{i1} \leq G_{i2} \leq \cdots \leq G_{im} = G_i \leq \cdots.$$

The Schreier Refinement Theorem (Cont'd)

- Similarly, there is a refinement of the second series arising from $N_{pq} = N_{p-1}(N_p \cap G_q)$,

$$\cdots \leq N_{p-1} = N_{p0} \leq N_{p1} \leq N_{p2} \leq \cdots \leq N_{pn} = N_p \leq \cdots$$

Both refinements have nm terms. For each i, j, the Zassenhaus Lemma gives

$$\frac{G_{i-1}(G_i \cap N_j)}{G_{i-1}(G_i \cap N_{j-1})} \cong \frac{N_{j-1}(N_j \cap G_i)}{N_{j-1}(N_j \cap G_{i-1})},$$

i.e., $G_{ij}/G_{i,j-1} \cong N_{ji}/N_{j,i-1}$.
Thus, the association $G_{ij}/G_{i,j-1} \mapsto N_{ji}/N_{j,i-1}$ is a bijection showing that the two refinements are equivalent.

The Jordan-Hölder Theorem

Theorem (Jordan-Hölder)

Let G be a finite group with $G \neq 1$. Then:

(1) G has a composition series;

(2) The composition factors in a composition series are unique, i.e., if $1 = N_0 \leq N_1 \leq \cdots \leq N_r = G$ and $1 = M_0 \leq M_1 \leq \cdots \leq M_s = G$, are two composition series for G, then $r = s$ and there is some permutation π of $\{1, 2, \ldots, r\}$, such that $M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}$, $1 \leq i \leq r$.

(1) This was shown in the preceding proposition.

(2) Suppose $1 = N_0 \leq N_1 \leq \cdots \leq N_r = G$ and $1 = M_0 \leq M_1 \leq \cdots \leq M_s = G$, are two composition series for G. By the Schreier Refinement Theorem, they have equivalent refinements, with rs terms. However, any refinement of a composition series is equivalent to the original composition series. Thus, the two compositions series must be equivalent.

The Fundamental Theorem of Arithmetic

Corollary

Every integer $n \geq 2$ has a factorization into primes. Moreover, the prime factors are uniquely determined by n.

- Since $\mathbb{Z}/n\mathbb{Z}$ is finite, it has a composition series. Let $G_1, G_2, \ldots, G_r$ be the composition factors. By a previous proposition, $n = |\mathbb{Z}/n\mathbb{Z}|$ is the product of the orders of its composition factors $n = \prod_{i=0}^{r} |G_i|$. Also, by a previous proposition, an abelian group is simple if and only if it is of prime order. So $|G_i|$ is prime, for all $1 \leq i \leq r$. We conclude that n is a product of primes.

  By Part (2) of the Jordan-Hölder Theorem, the (prime) orders of the composition factors are unique.

Solvable Groups

Definition (Solvable Group)

A group G is **solvable** if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G,$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, s-1$.

- The terminology comes from the correspondence in Galois Theory between these groups and polynomials solvable by radicals.
- It turns out that finite solvable groups are precisely those groups whose composition factors are all of prime order.

Solvability and Normal Subgroups

Proposition

Let G is a group and $N \trianglelefteq G$. If N and G/N are solvable, then so is G.

- Let $\overline{G} = G/N$ and, also,
  - $1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = N$ be a chain of subgroups of N, such that N_{i+1}/N_i is abelian, $0 \leq i < n$;
  - $\overline{1} = \overline{G_0} \trianglelefteq \overline{G_1} \trianglelefteq \cdots \trianglelefteq \overline{G_m} = \overline{G}$ be a chain of subgroups of $\overline{G}$ such that $\overline{G_{i+1}}/\overline{G_i}$ is abelian, $0 \leq i < m$.

  By the Lattice Isomorphism Theorem, there are subgroups G_i of G with $N \leq G_i$, such that $G_i/N = \overline{G_i}$ and $G_i \trianglelefteq G_{i+1}$, $0 \leq i < m$. By the Third Isomorphism Theorem, $\overline{G_{i+1}}/\overline{G_i} = (G_{i+1}/N)/(G_i/N) \cong G_{i+1}/G_i$. Thus,

  $$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = N = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$$

  is a chain of subgroups of G all of whose successive quotient groups are abelian. Therefore, G is solvable.

Subsection 5

Transpositions and the Alternating Group

Transpositions

- We saw (formal proof later) that every element of S_n can be written as a product of disjoint cycles in an essentially unique fashion.
- In contrast, every element of S_n can be written in many different ways as a (non disjoint) product of cycles.

  Example: Even in S_3 the element $\sigma = (1\ 2\ 3)$ may be written

  $$\sigma = (1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(1\ 3)(1\ 2)(1\ 3) = (1\ 2)(2\ 3).$$

  In fact, there are an infinite number of different ways to write σ.
- Not requiring the cycles to be disjoint destroys the uniqueness of a representation of a permutation as a product of cycles.
- We can, however, obtain a sort of "parity check" from writing permutations (non uniquely) as products of 2-cycles.

Definition (Transposition)

A 2-cycle is called a **transposition**.

Generation of S_n by Transpositions

- Every permutation of $\{1, 2, \ldots, n\}$ can be realized by a succession of transpositions or simple interchanges of pairs of elements:
  - First, note

    $$(a_1 \ a_2 \ldots a_m) = (a_1 \ a_m)(a_1 \ a_{m-1})(a_1 \ a_{m-2}) \cdots (a_1 \ a_2),$$

    for any m-cycle.
  - Now any permutation in S_n may be written as a product of cycles, e.g., its cycle decomposition.
  - Writing each of these cycles as a product of transpositions using the above procedure gives a product of transpositions.

Thus, we have $S_n = \langle T \rangle$, where $T = \{(i \ j) : 1 \leq i < j \leq n\}$.

Example: A Permutation as a Product of Transpositions

- Consider the permutation $\sigma \in S_{13}$, with

$$\begin{array}{lllll} \sigma(1)=12, & \sigma(2)=13, & \sigma(3)=3, & \sigma(4)=1, & \sigma(5)=11, \\ \sigma(6)=9, & \sigma(7)=5, & \sigma(8)=10, & \sigma(9)=6, & \sigma(10)=4, \\ \sigma(11)=7, & \sigma(12)=8, & \sigma(13)=2. & & \end{array}$$

  It can be written in disjoint cycle decomposition as:

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9).$$

  Therefore, as a product of transpositions,

$$\sigma = (1\ 4)(1\ 10)(1\ 8)(1\ 12)(2\ 13)(5\ 7)(5\ 11)(6\ 9).$$

The Polynomial Δ

- Even though, for a given $\sigma \in S_n$, there may be many ways of writing σ as a product of transpositions, we show that the parity (odd/even) is the same for any product of transpositions equaling σ.
- Let $x_1, \ldots, x_n$ be independent variables and let Δ be the polynomial

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j),$$

  i.e., the product of all the terms $x_i - x_j$, for $i < j$.

  Example: For $n = 4$,
  $\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$.
- For each $\sigma \in S_n$, let σ act on Δ by permuting the variables in the same way it permutes their indices: $\sigma(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$.

  Example: If $n = 4$ and $\sigma = (1\ 2\ 3\ 4)$, then
  $\sigma(\Delta) = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1)$.

The Sign Function ϵ

- Δ contains one factor $x_i - x_j$, for all $i < j$.
- Since σ is a bijection of the indices, $\sigma(\Delta)$ must contain either $x_i - x_j$ or $x_j - x_i$, but not both, for all $i < j$.
- If $\sigma(\Delta)$ has a factor $x_j - x_i$, where $j > i$, write this term as $-(x_i - x_j)$.
- Collecting all the changes in sign together we see that Δ and $\sigma(\Delta)$ have the same factors up to a product of -1's, i.e.,

$$\sigma(\Delta) = \pm\Delta, \text{ for all } \sigma \in S_n.$$

- For each $\sigma \in S_n$, let

$$\epsilon(\sigma) = \begin{cases} +1, & \text{if } \sigma(\Delta) = \Delta \\ -1, & \text{if } \sigma(\Delta) = -\Delta \end{cases}$$

Even and Odd Permutations

Example: In the previous example in S_4, with $\sigma = (1\ 2\ 3\ 4)$, we had

$$\begin{array}{rcl} \Delta & = & (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4) \\ \sigma(\Delta) & = & (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1). \end{array}$$

There are exactly 3 factors of the form $x_j - x_i$, where $j > i$, in $\sigma(\Delta)$, each of which contributes a factor of -1. Hence,

$$(1\ 2\ 3\ 4)(\Delta) = (-1)^3 \Delta = -\Delta.$$

Thus, $\epsilon((1\ 2\ 3\ 4)) = -1$.

Definition (Sign, Even and Odd Permutations)

(1) $\epsilon(\sigma)$ is called the **sign** of σ.

(2) σ is called **even** if $\epsilon(\sigma) = 1$ and **odd** if $\epsilon(\sigma) = -1$.

The Sign Function as a Homomorphism

Proposition

The map $\epsilon : S_n \to \{\pm 1\}$ is a homomorphism (where $\{\pm 1\}$ is a multiplicative version of the cyclic group of order 2).

- By definition, $(\tau\sigma)(\Delta) = \prod_{1 \leq i < j \leq n}(x_{\tau\sigma(i)} - x_{\tau\sigma(j)})$. Suppose that $\sigma(\Delta)$ has exactly k factors of the form $x_j - x_i$, with $j > i$, i.e., that $\epsilon(\sigma) = (-1)^k$. When calculating $(\tau\sigma)(\Delta)$, after first applying σ to the indices, we see that $(\tau\sigma)(\Delta)$ has exactly k factors of the form $x_{\tau(j)} - x_{\tau(i)}$, with $j > i$. Interchanging the order of the terms in these k factors introduces the sign change $(-1)^k = \epsilon(\sigma)$, and now all factors of $(\tau\sigma)(\Delta)$ are of the form $x_{\tau(p)} - x_{\tau(q)}$, with $p < q$. Thus, $(\tau\sigma)(\Delta) = \epsilon(\sigma)\prod_{1 \leq p < q \leq n}(x_{\tau(p)} - x_{\tau(q)})$. Since by definition of ϵ, $\prod_{1 \leq p < q \leq n}(x_{\tau(p)} - x_{\tau(q)}) = \epsilon(\tau)\Delta$, we obtain $(\tau\sigma)(\Delta) = \epsilon(\sigma)\epsilon(\tau)\Delta$, whence $\epsilon(\tau\sigma) = \epsilon(\sigma)\epsilon(\tau) = \epsilon(\tau)\epsilon(\sigma)$.

Example

- Let $n = 4$, $\sigma = (1\ 2\ 3\ 4)$ and $\tau = (4\ 2\ 3)$. Then $\tau\sigma = (1\ 3\ 2\ 4)$. By definition (using the explicit Δ in this case),

$$\begin{array}{rcl}(\tau\sigma)(\Delta) & = & (1\ 3\ 2\ 4)(\Delta) \\ & = & (x_3 - x_4)(x_3 - x_2)(x_3 - x_1)(x_4 - x_2)(x_4 - x_1)(x_2 - x_1) \\ & = & (-1)^5\Delta,\end{array}$$

where all factors except the first one are flipped to recover Δ. This shows $\epsilon(\tau\sigma) = -1$. On the other hand,

$$\begin{array}{rcl}(\tau\sigma)(\Delta) & = & \tau((x_2 - x_3)(x_2 - x_4)(x_2 - x_1) \\ & & \times (x_3 - x_4)(x_3 - x_1)(x_4 - x_1)) \\ & = & (x_{\tau(2)} - x_{\tau(3)})(x_{\tau(2)} - x_{\tau(4)})(x_{\tau(2)} - x_{\tau(1)}) \times \\ & & \times (x_{\tau(3)} - x_{\tau(4)})(x_{\tau(3)} - x_{\tau(1)})(x_{\tau(4)} - x_{\tau(1)}) \\ & = & (-1)^3 \prod_{1 \leq p < q \leq 4}(x_{\tau(p)} - x_{\tau(q)}) = (-1)^3\tau(\Delta).\end{array}$$

Since $\epsilon(\sigma) = (-1)^3 = -1$ and $\epsilon(\tau) = (-1)^2 = 1$, we verify $\epsilon(\tau\sigma) = -1 = \epsilon(\tau)\epsilon(\sigma)$.

Sign of Transpositions

- In $(1\ 2)(\Delta)$ only $(x_1 - x_2)$ will be flipped. So $(1\ 2)(\Delta) = -\Delta$, showing that $\epsilon((1\ 2)) = -1$.
- For any transposition $(i\ j)$, let λ be the permutation which interchanges 1 and i, interchanges 2 and j, and leaves all other numbers fixed (if $i = 1$ or $j = 2$, λ fixes i or j, respectively). Then, computing what $\lambda(1\ 2)\lambda$ does to any $k \in \{1, 2, \ldots, n\}$, we get $\lambda(1\ 2)\lambda = (i\ j)$. Since ϵ is a homomorphism, we obtain

$$\begin{aligned}\epsilon((i\ j)) &= \epsilon(\lambda(1\ 2)\lambda) = \epsilon(\lambda)\epsilon((1\ 2))\epsilon(\lambda) \\ &= (-1)\epsilon(\lambda)^2 = -1.\end{aligned}$$

Proposition

Transpositions are all odd permutations and ϵ is a surjective homomorphism.

The Alternating Groups

Definition (Alternating Group)

The **alternating group of degree** n, denoted by A_n, is the kernel of the homomorphism ϵ (i.e., the set of even permutations).

- By the First Isomorphism Theorem $S_n/A_n \cong \epsilon(S_n) = \{\pm 1\}$.
- The order of A_n is easily determined:

$$|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}(n!).$$

- $S_n - A_n$ is the coset of A_n which is not the identity coset. This is the set of all odd permutations.
- The signs of permutations obey the usual $\mathbb{Z}/2\mathbb{Z}$ laws:

$$\begin{aligned}(\text{even})(\text{even}) = (\text{odd})(\text{odd}) = \text{even};\\ (\text{even})(\text{odd}) = (\text{odd})(\text{even}) = \text{odd}.\end{aligned}$$

Uniqueness of Number of Transposition in Decomposition

- Since ϵ is a homomorphism and every $\sigma \in S_n$ is a product of transpositions, say $\sigma = \tau_1\tau_2\cdots\tau_k$, then $\epsilon(\sigma) = \epsilon(\tau_1)\cdots\epsilon(\tau_k)$.

  Since $\epsilon(\tau_k) = -1$, for $i = 1, \ldots, k$, $\epsilon(\sigma) = (-1)^k$.

  Thus, the parity of the number k is the same no matter how we write σ as a product: $\epsilon(\sigma) =$
  $$\begin{cases} +1, & \text{if } \sigma \text{ is a product of an even number of transpositions} \\ -1, & \text{if } \sigma \text{ is a product of an odd number of transpositions} \end{cases}.$$

Computing $\epsilon(\sigma)$ from the Cycle Decomposition of σ

- An m-cycle may be written as a product of $m-1$ transpositions. Thus, an m-cycle is an odd permutation if and only if m is even.

  For any permutation σ, let $\alpha_1\alpha_2\cdots\alpha_k$ be its cycle decomposition. Then $\epsilon(\sigma)$ is given by $\epsilon(\alpha_1)\cdots\epsilon(\alpha_k)$ and $\epsilon(\alpha_i)=-1$ if and only if the length of α_i is even. Hence, for $\epsilon(\sigma)$ to be -1 the product of the $\epsilon(\alpha_i)$'s must contain an odd number of factors of (-1).

Proposition

The permutation σ is odd if and only if the number of cycles of even length in its cycle decomposition is odd.

Example: $\sigma=(1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9)(10\ 11)(12\ 13\ 14\ 15)(16\ 17\ 18)$ has 3 cycles of even length, so $\epsilon(\sigma)=-1$.

Example: $\tau=(1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$ has exactly 2 cycles of even length, hence $\epsilon(\tau)=1$.

Parity of Order Versus Parity of Permutation

- Be careful not to confuse the terms "odd" and "even" for a permutation σ with the parity of the order of σ.
  - If σ is of odd order, all cycles in the cycle decomposition of σ have odd length so σ has an even (in this case 0) number of cycles of even length and hence is an even permutation.
  - If $|\sigma|$ is even, σ may be either an even or an odd permutation. E.g., (1 2) is odd, (1 2)(3 4) is even but both have order 2.