Artin: Groups

James Pagan

February 2024

Contents

1 Group Axioms

A **group** G is a set endowed with a binary operation, here denoted "$\times$", such that for all $a, b, c \in G$, the following four axioms are satisfied:

1. **Closure**: $ab \in G$.
2. **Associativity**: $a(bc) = (ab)c$.
3. **Identity**: There is $e \in G$ such that $ae = ea = a$.
4. **Invertability**: There is $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

If the operation is commutative — that is, if $ab = ba$ for all $a, b \in G$ — then G is said to be an **Abelian group**. The generalized associative law ensures that for all $a_1, \ldots, a_n \in G$, the product $a_1 \cdots a_n$ is independent of bracketing.

Theorem 1. *Let G be a group. Then the following properties hold for any $a, b \in G$:*

1. *The identity is unique.*
2. *Inverses are unique.*
3. $(a^{-1})^{-1} = a$.
4. $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. The proofs are as follows:

1. If e and f are identities of G, then $e = ef = f$ by the identity axiom.
2. If b and c are inverses of a — that is, $ab = ba = e = ac = ca$ — we have
$$b = be = b(ac) = (ba)c = ec = c.$$
3. As $a^{-1}(a^{-1})^{-1} = e$ and $aa^{-1} = e$,
$$a = ae = a(a^{-1}(a^{-1})^{-1}) = (aa^{-1})(a^{-1})^{-1} = e(a^{-1})^{-1} = (a^{-1})^{-1}.$$
4. Using the Generalized Associative Law, we have
$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$
$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e.$$
Thus $b^{-1}a^{-1}$ is $(ab)^{-1}$, the unique inverse of ab.

This completes the proof. $\square$

These axioms induce equation-like manipulations worth enumerating, for $a, b, c, d, x \in G$:

1. **Linear Equations**: If $ax = b$ or $xa = b$, multiplying by a^{-1} yields the unique solutions $x = a^{-1}b$ and $x = ba^{-1}$.
2. **Division**: If $ac = bc$ or $ca = ba$, we can multiply by c^{-1} to yield $a = b$.
3. **Multiplying Equations**: If $a = b$ and $c = d$, then $ac = bc$ and $bc = bd$ — hence $ac = bd$. Similarly, it implies $ad = bc$.

2 Subgroups and Cosets

2.1 Subgroups

A subset $H \subseteq G$ is a **subgroup** if it is a group under the operation of G.

Theorem 2. *If $H \subseteq G$ is nonempty, closed, and contains multiplicative inverses, it is a subgroup.*

Proof. Let $a \in H$. Since $a^{-1} \in H$ too, we have $e = a^{-1}a \in H$ — thus H contains a multiplicative identity. Multiplication is associative for all elements of H (as elements of G), so the axioms are indeed verified. $\square$

A group is **finite** if G contains finitely many elements and **infinite** otherwise. If G is a finite group, the **order** of G — denoted $|G|$ — is the number of elements of G.

Theorem 3. *Suppose G is finite. If $H \subseteq G$ is nonempty and closed, it is a subgroup.*

Proof. Let $|G| = n$ and select $a \in H$. Consider the list

$$a,\ a_2,\ \ldots,\ a^n,\ a^{n+1}.$$

Since this list in G (a set with n elements) contains $n + 1$ elements, the Pigeonhole Principle guarantees that there exist $i, j \in \{1, \ldots, n + 1\}$ with $i < j$ such that

$$a^i = a^j.$$

Then $a^{i-j} = e$, and $a^{-1} = a^{i-j-1} \in H$ by closure. Hence H contains multiplicative inverses, so Theorem 2 establishes that H is a subgroup. $\square$

The subgroup relation is transitive. If M is a subgroup of H and H is a subgroup of G, then M is a subgroup of G.

2.2 Cosets and Lagrange's Theorem

Let $H \subseteq G$ be a subgroup. Then for $a \in G$, the **left coset** aH and **right coset** Ha are defined as follows:

$$aH = \{ah \mid h \in H\} \qquad \text{and} \qquad Ha = \{ha \mid h \in H\}.$$

For the remainder of this document, "coset" will refer to left cosets unless otherwise specified. Realize that $b \in aH$ if and only if $a^{-1}b \in H$. Thus for $a, b \in G$, the relation $a \sim b$ if $a^{-1}b \in H$ biconditionally implies that a and b lie in some common coset.

Theorem 4. *Let $H \subseteq G$ be a subgroup. Then the relation $a \sim b$ for $a, b \in G$ is an equivalence relation.*

Proof. We must verify three properties, for all $a, b, c \in G$:

1. **Reflexivity**: We have that $a^{-1}a = e \in H$, so $a \sim a$.
2. **Symmetry**: This follows from the fact H contains inverses:

$$a \sim b \iff a^{-1}b \in H \iff b^{-1}a \in H \iff b \sim a.$$

3. **Transitivity**: Suppose that $a \sim b$ and $b \sim c$ — that is, $a^{-1}b$ and $b^{-1}c$ lie in H. Then

$$a^{-1}c = a^{-1}ec = (a^{-1}b)(b^{-1}c) \in H;$$

thus we find $a \sim c$.

We conclude that $\sim$ is an equivalence relation. $\square$

It is easy to demonstrate that equivalence classes are cosets themselves, which leads to a sharper proof of the following Theorem:

Theorem 5. *Suppose that $a, b \in G$ and $H \subseteq G$ is a subgroup. Then $aH = bH$ or $aH \cap bH = \varnothing$.*

Proof. Suppose that $aH \cap bH \neq 0$; then there exists $c \in G$ and $h_1, h_2 \in H$ such that

$$c = ah_1 = bh_2.$$

Thus the conversion factors $a = bh_2h_1^{-1}$ and $b = ah_1h_2^{-1}$ imply that all elements of aH are elements of bH and vice versa. We conclude that $aH = bH$. $\square$

Theorem 6. *For all $a \in G$, we have $|aH| = |H|$.*

Proof. Define a *mapping* $\phi : aH \to H$ by the rule $f(ah) = h$. We wish to prove that f is a bijection.

1. **Injectivity**: Suppose that $f(ah_1) = f(ah_2)$ — that is, $h_1 = h_2$. Multiplying by a yields $ah_1 = ah_2$.
2. **Surjectivity**: For all $h \in H$, we have that $f(ah) = h$.

Hence f is bijective. We conclude that $|aH| = |H|$. □

Therefore, the cosets of H partition the group G into equivalence classes of size $|H|$. For this reason, we sometimes denote aH by $[a]$.

Theorem 7 (Lagrange's Theorem)**.** *Let H be a subgroup of the finite group G. Then the order of H divides the order of G.*

Proof. Let the distinct cosets of H be $a_1H, \ldots, a_kH$ for $a_1, \ldots, a_k \in G$; then

$$a_1H \cap \cdots \cap a_kH \;=\; G.$$

If we let $|H| = m$ and $|G| = n$, the above formula implies that $mk = n$ and $m \mid n$. □

There are two more trivial assertions that bear coset manipulation a striking resemblance to manipulation of elements:

1. $a(bH) = (ab)H$ and $(Ha)b = H(ab)$.
2. $aH = bH$ if and only if $H = a^{-1}bH$.

2.3 Normal Subgroups

A subgroup $N \subseteq G$ is **normal** if $aN = Na$ for all $a \in G$. Equivalently, N is normal if $aNa^{-1} = N$ or if $ana^{-1} \in N$ for each $n \in N$. This relation is denoted $N \lhd G$. All groups have at least two normal subgroups: G itself and the **trivial group**, $\{e\}$.

Normality is *not* transitive. $M \lhd N$ and $N \lhd G$ does not always entail that $N \lhd G$.

2.4 Quotient Groups

Suppose $N \lhd G$. Then the **quotient group** $G\,/\,N$ is the group of equivalence classes $[a] = aN$ under the operation $[a][b] = [ab]$ or equivalently $aN \times bN = abN$.

Theorem 8. *Let $N \lhd G$. Then $G\,/\,N$ is a group.*

Proof. Suppose that N is normal. We first prove that $\times$ is well-defined; let $aN = bN$ and $cN = dN$. Then

$$aNc = bNc \implies acN = bcN \qquad \text{and} \qquad bcN = bdN,$$

so $acN = bdN$. It is clear that $G\,/\,N$ is closed and associative by the relevant properties of G. The identity of $G\,/\,N$ is N itself, since

$$aN \times N \;=\; aN \times eN \;=\; (ae)N \;=\; N \;=\; (ea)N \;=\; eN \times aN \;=\; N \times aN.$$

Finally, $G\,/\,N$ contains inverses: we have

$$aN \times a^{-1}N = (aa^{-1})N = eN = N = eN = (a^{-1}a)N = a^{-1}N \times aN.$$

Thus the inverse of aN is $a^{-1}N$. We conclude that $G\,/\,N$ is a group. $\square$

Indeed, $G\,/\,N$ is a group if and *only* if N is normal:

Theorem 9. *Let $H \subseteq G$ be a subgroup. If $G\,/\,H$ is a group, then H is normal.*

Proof. Select $h \in H$ arbitrarily. For all $a \in G$, we have that $[ah] = [a]$; thus

$$[e] = [a^{-1}a] = [a^{-1}][a] = [a^{-1}][ah] = [a^{-1}ha].$$

Hence $a^{-1}ha \in H$. We deduce that H is a normal subgroup. $\square$

The **canonical epimorphism** $\pi : G \to G\,/\,N$ is the surjective homomorphism defined by $\pi(a) = aN$. It is clear that π is a homomorphism, since

$$\pi(ab) \;=\; abN \;=\; aN \times bN \;=\; \pi(a)\pi(b).$$

Applying the Correspondence Theorem to the canonical surjection yields that subgroups in $G\,/\,N$ correspond one-to-one with subgroups in G that contain N.

3 Homomorphisms

3.1 Definition

A **group homomorphism** between two groups G and H is a mapping $\phi : G \to H$ such that for all $a, b \in G$,

$$\phi(ab) = \phi(a)\phi(b).$$

There are several types of homomorphisms to consider:

1. A surjective homomorphism is an **epimorphism**, an injective homomorphism is a **monomorphism**, and a bijetive homomorphism is an **isomorphism**.
2. A homomorphism $\phi : G \to G$ is an **epimorphism**, and an isomorphic epimorphism is an **automorphism**.

If there exists an isomorphism between G and H, their structures are equivalent: we say G and H are **isomorphic** and write $G \cong H$.

Theorem 10. *If $\phi : G \to H$ is a homomorphism, then the following properties hold for all $a \in G$:*

1. $\phi(e_G) = e_H$.

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

Proof. Let us divide our proof into two parts:

1. Let $a \in G$. Then $\phi(e_G)\phi(a) = \phi(e_G a) = \phi(a)$. Multiplying by $\phi(a)^{-1}$ yields that $\phi(e_G) = e_H$.
2. We have that

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_G) = e_H = \phi(e_G) = \phi(a^{-1}a) = \phi(a^{-1})\phi(a).$$

   The uniqueness of inverses in H ensures that $\phi(a)^{-1} = \phi(a^{-1})$.

This completes the proof. □

3.2 Kernel, Image, Cokernel

Let $\phi : G \to H$ be a homomorphism. The structure of this homomorpism is encapsulated by three different groups:

1. **Kernel**: The set $\operatorname{Ker}\phi = \{k \mid \phi(k) = e\}$.
2. **Image**: The set $\operatorname{Im}\phi = \{\phi(a) \mid a \in G\}$, often denoted $\phi(G)$.

If $\operatorname{Im}\phi$ is a normal subgroup, then the **cokernel** of ϕ is the quotient group $\operatorname{Coker}\phi = H \,/\, \operatorname{Im}\phi$. This object is only explored when H is an Abelian group.

Theorem 11. *Let $\phi : G \to H$ be a homomorphism. Then the folowing two results hold:*

1. $\operatorname{Ker}\phi$ *is a normal subgroup of* G.
2. $\operatorname{Im}\phi$ *is a subgroup of* H.

Proof. $\operatorname{Ker}\phi$ is nonempty since $\phi(e) = e$. We now verify that $\operatorname{Ker}\phi$ is normal:

1. **Closure**: If $a, b \in \operatorname{Ker}\phi$, then $\phi(a) = \phi(b) = e$; therefore $\phi(ab) = \phi(a)\phi(b) = e$, so $ab \in \operatorname{Ker}\phi$.
2. **Invertability**: Suppose $\phi(a) \in \operatorname{Ker}\phi$. Then $\phi(a^{-1}) = \phi(a)^{-1} = e^{-1} = e$, so $a^{-1} \in \operatorname{Ker}\phi$
3. **Normality**: Let $k \in \operatorname{Ker}\phi$ and $a \in G$. Then

$$\phi(a^{-1}ka) = \phi(a)^{-1}\phi(k)\phi(a) = \phi(a)^{-1}\phi(a) = e;$$

hence $a^{-1}ka \in \operatorname{Ker}\phi$. We conclude that $\operatorname{Ker}\phi$ is normal.

Thus $\operatorname{Ker}\phi$ is a normal subgroup. Since it is clear that $\operatorname{Im}\phi$ is nonempty, we must verify:

1. **Closure**: If $\phi(a), \phi(b) \in \operatorname{Im}\phi$, then we have $\phi(a)\phi(b) = \phi(ab) \in \operatorname{Im}\phi$.
2. **Invertability**: If $\phi(a) \in \operatorname{Im}\phi$, then we have $\phi(a)^{-1} = \phi(a^{-1}) \in \operatorname{Im}\phi$.

We conclude that $\operatorname{Im}\phi$ is a subgroup. This completes the proof. □

The reason normal subgroups are critical is precisely because the kernel of ϕ is normal.

Theorem 12. *Let $\phi : G \to H$ be a homomorphism. The following two theorems hold:*

1. *ϕ is a monomorphism if and only if* $\operatorname{Ker}\phi = \{e\}$.
2. *ϕ is an epimorphism if and only if* $\operatorname{Im}\phi = H$.

Proof. Suppose that ϕ is a monomorphism. Thus

$$\phi(a) = e \implies \phi(a) = \phi(e) \implies a = e,$$

so $\operatorname{Ker}\phi = \{e\}$. If we suppose that $\operatorname{Ker}\phi = \{e\}$, we have that

$$\phi(a) = \phi(b) \implies \phi(ab^{-1}) = e \implies ab^{-1} = e \implies a = g,$$

so ϕ is a monomorphism. The story with epimorphisms is quite simple. □

The following theorem explores a special case of the Correspondence Theorem.

Theorem 13. *Let* $\operatorname{Ker}\phi = K$. *Then $a \in G$ implies $\{b \mid \phi(b) = \phi(a)\} = aK$.*

Proof. We utilize the following chain of equivalencies:

$$\phi(b) = \phi(a) \iff \phi(ba^{-1}) = e \iff ba^{-1} \in K \iff b \in aK.$$

We conclude the desired set equality: □

3.3 The Isomorphism Theorems

For the remainder of this section, let $\phi : G \to H$ be a homomorphism.

Theorem 14 (First Isomorphism Theorem)**.** $G \,/\, \operatorname{Ker}\phi \cong \operatorname{Im}\phi$.

Proof. Let $K = \operatorname{Ker}\phi$, and define a morphism $\psi : G\,/\,K \to \operatorname{Im}\phi$ by $\psi(aK) = \phi(a)$. We have for arbitrary $a, b \in G$ that

$$\psi(aK \times bK) \;=\; \psi(abK) \;=\; \pi(ab) \;=\; \phi(a)\phi(b) \;=\; \psi(aK)\psi(bK).$$

Hence ψ is a homomorphism. For injectivity, suppose that $\Psi(aK) = \Psi(bK)$ — that is, $\phi(a) = \phi(b)$. Then

$$\phi(a^{-1}b) \;=\; \phi(a)^{-1}\phi(b) \;=\; e_H,$$

so $a^{-1}b \in K$. Thus $aK = bK$. For surjectivity, it is clear that for all $\phi(a) \in \operatorname{Im}\phi$ we have $\psi(aK) = \phi(a)$. We conclude that ψ is the desired isomorphism. □

Let $\phi : G \to H$ be a homomorphism. Here are two special cases of the prior theorem:

1. If ϕ is a monomorphism, them $G \cong \operatorname{Im} \phi$.
2. If ϕ is an epimorphism, then $G \,/\, \operatorname{Ker} \phi \cong H$.

For a subgroup $M' \subseteq H$, define the **contraction group** $M = \{a \in G \mid \phi(a) \in M'\}$. This terminology is self-invented, but mirrors the contraction and extension of ideals.

Theorem 15 (Correspondence Theorem)**.** *Subgroups of G which contain $\operatorname{Ker} \phi$ correspond one-to-one with subgroups of H.*

Proof. □