

Math 551 – Algebra – Fall 2002

Richard Lyons
Rutgers University
New Brunswick, New Jersey, USA

A. Groups

3. The Meat-Axe: Noether Isomorphism Theorems and the Jordan-Hölder Theorem

If $K \triangleleft G$, then G is broken up (in some way) into the groups K and G/K . In general G cannot be recovered just from K and G/K (for example, both $G = \mathbf{Z}_2 \times \mathbf{Z}_2$ and $G = \mathbf{Z}_4$ have subgroups $K \cong \mathbf{Z}_2$ such that $G/K \cong \mathbf{Z}_2$, though $\mathbf{Z}_4 \not\cong \mathbf{Z}_2 \times \mathbf{Z}_2$). Nevertheless the pair K and G/K contain a significant amount of information about the structure of G , and we pursue this idea in this section. For instance, if $H \leq G$, how does the “cut” K cut through H ? And if $H \triangleleft G$ how does it cut through G/H ? What happens if we cut up a group G “as much as possible”, and is there indeed a maximal way to do it?

3a. The Noether Isomorphism Theorems

We begin with the three fundamental isomorphism theorems often named for Emmy Noether, the cigar-smoking pioneer of “modern” algebra.

Theorem. (*First Isomorphism Theorem*) Let $\phi : G \rightarrow H$ be a homomorphism of groups, and let $K = \ker \phi$. Then there exists a unique isomorphism $\bar{\phi} : G/K \rightarrow \phi(G)$ such that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ \downarrow & & \uparrow \\ G/K & \xrightarrow{\bar{\phi}} & \phi(G) \end{array}$$

Here the mapping on the left is π_K and the mapping on the right is the inclusion of $\phi(G)$ in H .

Proof. In fact there is a unique mapping $\bar{\phi}$ such that the diagram commutes; the only possibility is to define $\bar{\phi}(gK) = \phi(g)$. Since $\phi(g) = \phi(g')$ whenever $gK = g'K$, this is well-defined. Moreover $\bar{\phi}(gKg'K) = \bar{\phi}(gg'K) = \phi(gg') = \phi(g)\phi(g') = \bar{\phi}(gK)\bar{\phi}(g'K)$ so $\bar{\phi}$ is a homomorphism. Clearly $\phi(G) = \bar{\phi}(G/K)$ so $\bar{\phi}$ is surjective; also $gK \in \ker \bar{\phi} \iff \phi(g) = 1 \iff g \in \ker \phi = K \iff gK = K$, so $\bar{\phi}$ is injective. Hence $\bar{\phi}$ is an isomorphism.

□

Corollary. *If ϕ is any homomorphism from G to H , then $G/\ker \phi \cong \phi(G)$. If ϕ is surjective, then $G/\ker \phi \cong H$.*

1. Let $H \leq G$. Then we obtain a homomorphism $\phi : G \rightarrow \Sigma_{G/H}$ whose image is transitive on G/H and whose kernel is $K = \bigcap_{g \in G} gH$. In particular $K \leq H$ and G/K is isomorphic to a transitive subgroup of $\Sigma_{G/H}$.
2. Applying this to $G \cong \Sigma_4$ and $H \in \text{Syl}_2(G)$, we have $|H| = 8$ so $|G : H| = 3$. We get a homomorphism $\Sigma_4 \rightarrow \Sigma_3$ whose image I is transitive and whose kernel K is a normal subgroup such that $\Sigma_4/K \cong I$. The only possibility is $K = V$, and so $\Sigma_4/V \cong \Sigma_3$.

Theorem. *(Second Isomorphism Theorem, or Parallelogram Law) Let H and K be subgroups of G and suppose that $H \leq N_G(K)$. Then $HK \leq G$, $K \triangleleft HK$ and $H \cap K \triangleleft H$, and*

$$H/H \cap K \cong HK/K$$

via the isomorphism $h(h \cap K) \mapsto hK$ ($h \in H$).

Proof. We are given that ${}^hK = K$ for all $h \in H$, so that $hK = Kh$ for all such h . Therefore $HK = KH$, which implies as before that $HK \leq G$: $(HK)(HK) = H(KH)K = H(HK)K = HHKK = HK$, etc. Moreover, $N_{HK}(K)$ is a subgroup of HK containing K and H , so equals HK , and so $K \triangleleft HK$. Now consider the homomorphism which is the composite of the inclusion and the canonical projection:

$$\phi : H \rightarrow HK \rightarrow HK/K.$$

For any $h \in H$ and $k \in K$, we have $hkkK = hK = \phi(h)$, so ϕ is surjective. Moreover for any $h \in H$, we have $h \in \ker \phi \iff hK = K \iff h \in K \iff h \in H \cap K$, so $\ker \phi = H \cap K$. The first isomorphism theorem then implies that the mapping

$$\bar{\phi} : H/H \cap K \rightarrow HK/K \text{ taking } h(H \cap K) \mapsto hK$$

is an isomorphism. QED

Corollary. *Suppose that $K \triangleleft G$ and H is a subgroup of G such that $H \cap K = 1$. Then G/K has a subgroup isomorphic to H . Moreover if $HK = G$ then $G/K \cong H$.*

However, if $K \triangleleft G$ it is not necessarily the case that $H \cap K = 1$ for any nontrivial subgroup of G , let alone that $H \cap K = 1$ and $G = HK$ for some H (in which case we say that G splits over K). For instance, in $G = Z_4$, there is a unique subgroup K of order 2, but there is no subgroup H of G such that $H \cap K = 1$, other than the trivial subgroup $H = 1$.

Theorem. *(The Third Isomorphism Theorem, or the Correspondence Theorem) Let $\phi : G \rightarrow H$ be a **surjective** homomorphism, and let $K = \ker \phi$. Let \mathcal{S} be the set of all subgroups of G containing K , and let \mathcal{T} be the set of all subgroups of H . Then*

- 1) For each $S \in \mathcal{S}$, $\phi(S) \in \mathcal{T}$; and for each $T \in \mathcal{T}$, $\phi^{-1}(T) \in \mathcal{S}$.

- 2) The mappings $S \mapsto \phi(S)$ and $T \mapsto \phi^{-1}(T)$ are mutually inverse bijections between \mathcal{S} and \mathcal{T} .
- 3) These bijections have the following further properties, for all $S, S' \in \mathcal{S}$ and $T, T' \in \mathcal{T}$:
- $S \leq S'$ if and only if $\phi(S) \leq \phi(S')$, and if these conditions hold then $|S' : S| = |\phi(S') : \phi(S)|$;
 - $S \triangleleft S'$ if and only if $\phi(S) \triangleleft \phi(S')$, and if these conditions hold then $S'/S \cong \phi(S')/\phi(S)$;
 - $\phi(S \cap S') = \phi(S) \cap \phi(S')$.
 - $\phi(\langle S, S' \rangle) = \langle \phi(S), \phi(S') \rangle$.

Proof. 1) is obvious (note that $\phi^{-1}(T) \supseteq \phi^{-1}(1) = \ker \phi = K$). To prove 2) we must show that $\phi(\phi^{-1}(T)) = T$ and $\phi^{-1}(\phi(S)) = S$ for all $S \in \mathcal{S}$ and $T \in \mathcal{T}$. The first is a property of any surjective mapping of sets. As for the second, it is automatic from the definition of ϕ^{-1} that $S \subseteq \phi^{-1}(\phi(S))$. Let $x \in \phi^{-1}(\phi(S))$. Then $\phi(x) \in \phi(S)$ so $\phi(x) = \phi(y)$ for some $y \in S$. Then $xy^{-1} \in \ker \phi = K \leq S$ (recall $S \in \mathcal{S}$!). Hence $x = xy^{-1}y \in S$, proving 2).

The first and third statements of 3) are left to the reader. (For the statement about indices, check that $g_1S = g_2S \iff \phi(g_1)\phi(S) = \phi(g_2)\phi(S)$, the converse statement requiring S to contain $\ker \phi$. As for 3b), if $S \triangleleft S'$, then for every $x \in S$ and $g \in S'$, an equation of the form $\cong gx = y$ holds for some $y \in S'$. Hence the image of this equation under ϕ is also true, whence $\phi(S) \triangleleft \phi(S')$. Conversely suppose that $\phi(S) \triangleleft \phi(S')$. Then the composite of $\phi|_{S'}$ and the canonical projection

$$\psi : S' \rightarrow \phi(S') \rightarrow \phi(S')/\phi(S)$$

is a homomorphism; both pieces are surjective so ψ is also surjective. Moreover $x \in \ker \psi \iff \phi(x) \in \phi(S) \iff x \in \phi^{-1}\phi(S) = S$, so by the first isomorphism theorem $S \triangleleft S'$ and $S'/S \cong \phi(S')/\phi(S)$. QED

Corollary. If $H \leq K \leq G$ with $H \triangleleft G$ and $K \triangleleft G$, then $K/H \triangleleft G/H$, and $G/H \Big/ K/H \cong G/K$.

The proof is left to the reader.

These theorems answer the question above about how a normal subgroup $K \triangleleft G$ cuts through a subgroup H of G or through a quotient G/H of G . Namely if $H \leq G$, then $H \cap K \triangleleft H$, and $H \cap K$ is a subgroup of K , while $H/H \cap K$ is isomorphic to a subgroup of G/K . On the other hand if $H \triangleleft G$, then $HK \triangleleft G$ (easy to check), so $HK/H \triangleleft G/H$, with $HK/H \cong K/H \cap K$ isomorphic to a quotient of K and $G/H \Big/ HK/H \cong G/HK \cong G/K \Big/ HK/K$ isomorphic to a quotient of G/K .

3b. Groups with operators

We pause to broaden the scope of this discussion, which has an almost trivial extension to a slightly more complex situation, and as a result the theory extends without essential change to vector spaces and modules, instead of just groups. The key notion is that of a **group with operators**, which consists of a group G and a set S which operates on G , but not in the sense of group action (for S itself need not be a group or indeed have any structure beyond that of a set). Instead, the only axiom is that the operators from S preserve the group structure on G .

Definition. Let G be a group and S a set. We say that G is an S -group (or a group with operators S) if there is defined a function

$$S \times G \rightarrow G, \text{ taking } (s, g) \mapsto sg,$$

such that $s(gh) = (sg)(sh)$ for all $s \in S$ and $g, h \in G$. Moreover, a subgroup $H \leq G$ is called an S -subgroup of G if and only if $sg \in H$ for all $s \in S$ and $g \in H$. If G and H are S -groups (for the same S) then a mapping $\phi : G \rightarrow H$ is an S -homomorphism (resp. S -isomorphism) if and only if it is a homomorphism (resp. isomorphism) of groups and $\phi(sg) = s\phi(g)$ for all $s \in S, g \in G$. The two S -groups G and H are S -isomorphic if and only if there exists an S -isomorphism from one to the other.

The exponential notation g^s in place of sg is perhaps more suggestive, since the axiom for a group with operators then becomes

$$(gh)^s = g^s h^s.$$

Ex. A. Let V be a vector space over \mathbf{C} (or more generally over any field F). The axioms for a vector space prescribe that V is an abelian group with respect to addition, and also that several axioms hold concerning scalar multiplication, so that V is a \mathbf{C} -group (or an F -group), with respect to the operations of addition and scalar multiplication. Then a \mathbf{C} -subgroup (or F -subgroup) of V is nothing other than a subspace; and a \mathbf{C} -homomorphism (\mathbf{C} -isomorphism) between two vector spaces is just a linear transformation (isomorphism of vector spaces). We then immediately get from the first theorem that if $T : V \rightarrow W$ is a linear transformation of vector spaces, then $V/\ker(T) \cong \text{im}(T)$ (as vector spaces), which immediately gives e.g. the “rank plus nullity” theorem: $\dim \ker(T) + \dim \text{im}(T) = \dim V$. Likewise the second theorem gives $(W + X)/W \cong X/(W \cap X)$ for all subspaces W, X of a vector space V , and the third theorem implies that given a subspace W of a vector space V , the set of subspaces of V containing W is in one-to-one correspondence with the set of subspaces of V/W ; also for $W \leq X \leq V$, $V/X \cong (V/W)/(X/W)$.

Ex. A'. Let M be a module over a ring R (same axioms as for a vector space, except that the scalars come from a ring R instead of from a field).

Ex. B. Let G be a group and consider G as a G -group via the definition

$$g \cdot h = {}^g h \quad \forall g, h \in G.$$

Then the G -subgroups of G are the normal subgroups of G . A G -homomorphism from G to G is a homomorphism ϕ such that $g(\phi(h)) = \phi(g)(\phi(h))$ for all $g, h \in G$. In particular the image of such a homomorphism is a normal subgroup of G , which is ordinarily not the case for homomorphisms.

Ex. B'. Any group G can be considered an $\text{Aut}(G)$ -group via $\alpha \cdot g = \alpha(g)$. The $\text{Aut}(G)$ -subgroups of G are called the characteristic subgroups of G . E.g., $Z(G)$ is a characteristic subgroup of G .

Notice that this is also an action of $\text{Aut}(G)$ on G , i.e., $\alpha\beta(g) = \alpha(\beta(g))$. Thus for any characteristic subgroup N of G we obtain a homomorphism

$$\text{Aut}(G) \rightarrow \text{Aut}(N), \alpha \mapsto \alpha|_N.$$

Ex. C. Let Γ be a group and V a vector space over a field F . A representation of Γ on V is a homomorphism

$$\phi : \Gamma \rightarrow GL(V).$$

Such a homomorphism amounts to the structure of a Γ -group on V , by which Γ acts on V ; the connection being

$$g \cdot v = \phi(g)(v),$$

Thus we may consider V to be a $\Gamma \cup F$ -group. The usual notion of equivalence of representations is just the notion of $\Gamma \cup F$ -isomorphism. That is, representations of Γ on V and W if and only if there exists an invertible abelian group homomorphism $V \rightarrow W$ preserving the actions of both Γ and F ; i.e., a nonsingular linear transformation preserving the action of Γ . The representation is irreducible if and only if V is a simple $\Gamma \cup F$ -group.

Notice that given a representation $\phi : \Gamma \rightarrow V$, if W is a $\Gamma \cup F$ -subgroup of V , then both W and V/W are $\Gamma \cup F$ -groups and so give representations of Γ as well.

3c. Normal series and the Theorem of Jordan and Hölder

Definition. A (S) -group $G \neq \{1\}$ is a simple (S) -group if and only if there exist no normal (S) -subgroups of G other than 1 and G itself.

In other words simplicity is equivalent to having no nontrivial quotients. We have seen that A_n is simple for $n \geq 5$.

Now let G be a (S) -group. In the case $G = 1$ there is nothing to discuss, so assume that $G \neq 1$. If G is not simple then there exists a proper normal (S) -subgroup H , and so

$$1 \triangleleft H \triangleleft G.$$

If H and G/H are both (S) -simple we can stop; but otherwise a further term may be inserted, either between 1 and H , or between H and G , by the Correspondence Theorem:

$$1 \triangleleft K \triangleleft H \triangleleft G \text{ or } 1 \triangleleft H \triangleleft K \triangleleft G.$$

If the three corresponding quotients are (S -)simple, we stop; otherwise we can insert a further term somewhere, and so on.

If this process stops after finitely many steps we reach a series

$$1 = G_n \triangleleft_{\neq} G_{n-1} \triangleleft_{\neq} \cdots \triangleleft_{\neq} G_2 \triangleleft_{\neq} G_1 \triangleleft_{\neq} G_0 = G \quad (3A)$$

in which

$$\text{the quotients } G_0/G_1, G_1/G_2, \dots, G_{n-1}/G_n \text{ are all } (S)\text{-simple.} \quad (3B)$$

Equivalently it is a series in which no further terms may be inserted to produce another “normal” series. Such a series (3A) satisfying (3B) is called a (S -)composition series of G .

Definition. A normal series for a (S -)group G is a finite series as in (3A) (but not necessarily satisfying (3B)). The integer n is the length of the series, and the quotients in (3B) are the factors of the series. If the factors are all (S -)simple, then the normal series is called a (S -)composition series and its factors are called the composition factors of G .

The Jordan-Hölder Theorem will justify calling the factors “the” composition factors of G .

One obvious sufficient condition for G to possess a composition series is that G be finite. Another is that G possess both the maximum and minimum condition on subgroups[†]: that is, there exist no infinite ascending chains or descending chains of subgroups of G :

$$H_1 \not\leq H_2 \not\leq \cdots \not\leq H_n \not\leq \cdots \leq G \text{ or } G \geq H_1 \geq H_2 \geq \cdots \geq H_n \geq \cdots$$

For if G satisfies these conditions, then G must possess a maximal (S -)normal subgroup G_1 . (Choose any normal subgroup M_1 . If this is not maximal, we get $M_1 \not\leq M_2$ for some normal M_2 . If M_2 is not maximal, we get $M_1 \not\leq M_2 \not\leq M_3$ and this process must terminate by the maximum condition.)

Then G/G_1 is (S -)simple by the maximality of G_1 . Moreover G_1 inherits the maximum condition, so possesses a maximal normal subgroup G_2 , and continuing we obtain a composition series

$$1 \triangleleft_{\neq} G_{n-1} \triangleleft_{\neq} \cdots \triangleleft_{\neq} G_2 \triangleleft_{\neq} G_1 \triangleleft_{\neq} G,$$

the process terminating by the minimum condition.

Examples of infinite S -groups satisfying these conditions are finite-dimensional vector spaces (with S being the field of scalars).

The main thrust of the Jordan-Hölder Theorem is the uniqueness statement. We say that two normal series of G , say (3A) and

$$1 = H_{n'} \triangleleft_{\neq} H_{n'-1} \triangleleft_{\neq} \cdots \triangleleft_{\neq} H_2 \triangleleft_{\neq} H_1 \triangleleft_{\neq} H_0 = G, \quad (3C)$$

are *equivalent* if and only if $n = n'$ and the two lists

$$G_0/G_1, G_1/G_2, \dots, G_{n-1}/G_n \text{ and } H_0/H_1, H_1/H_2, \dots, H_{n'-1}/H_{n'}$$

of composition factors can be reordered so that corresponding terms are (S -)isomorphic.

[†] Actually there is a weaker sufficient condition: that G possess the maximum and minimum condition on subnormal subgroups. A subgroup of G is subnormal in G if and only if it is a term in some normal series for G .

Theorem (Jordan and Hölder). *Let G be an S -group. Then the following conditions hold.*

E) If G is finite, or more generally possesses the maximum and minimum conditions on subgroups, then G possesses a (S -)composition series; moreover any (S -)normal series may be “refined” by the suitable addition of new terms to a (S -)composition series.

U) Any two (S -)composition series are equivalent.

Proof. We have already proved the first existence statement. The second follows by a similar argument.

A slightly stronger statement than the uniqueness statement is easier to prove. It is the following:

Theorem. *Suppose that G has a composition series (3A) (of length n) and also has a normal series (3C) of length $n' \geq n$. Then the series (3C) is a composition series, $n' = n$, and the two composition series are equivalent.*

This implies the Jordan-Hölder uniqueness statement, since given two composition series, of length n and n' , we may assume without loss that $n' \geq n$, and then the theorem gives us what we want (a composition series is a certain kind of normal series).

Proof Let series (3A), (3C) be given as assumed in the theorem. We go by induction on n . We consider two cases.

Case 1. $H_1 \leq G_1$. In this case by inserting the term G_1 in the series (3C) (unless it was there already, as H_1), we get a series, call it (3C'), which is like (3C) but of length n' or $n' + 1$, and with the next-to-top term G_1 . From G_1 down, the series (3A) and (3C') give a composition series of G_1 of length $n - 1$, and a normal series of length $n' - 1$ or n' . Since $n' - 1 \geq n - 1$, induction implies that these two series for G_1 are equivalent, and both have length $n - 1$. Therefore (3C') had length n , which implies that (3C) had length n and $H_1 = G_1$. Now the composition factors of (3A) and (3C) are obtained from those of our two composition series for G_1 just by appending the one further group $G/G_1 = G/H_1$, so we are done in this case.

Case 2. $H_1 \not\leq G_1$. Therefore $G_1H_1 > G_1$. But G_1 is a maximal normal subgroup of G since (3A) is a composition series. Therefore $G_1H_1 = G$ (as $G_1H_1 \triangleleft G$). We set

$$K_2 = G_1 \cap H_1 \triangleleft G.$$

We get a parallelogram with G at the top, K_2 at the bottom and G_1 and H_1 the other two vertices. By the second isomorphism theorem,

$$G/G_1 \cong H_1/K_2 \text{ and } G/H_1 \cong G_1/K_2.$$

We now construct a normal series (C) for K_2 as follows. If possible, construct a composition series (C) for K_2 . Otherwise following the procedure described at the beginning of this

section we obtain normal series of arbitrary length; we choose (C) to have length $n - 1$ (anything larger would do just as well).

Then the two series

$$1 = G_n \not\leq G_{n-1} \not\leq \cdots \not\leq G_1 \text{ and } \cdots (C) \cdots K_2 \not\leq G_1$$

are a composition series for G_1 of length $n - 1$ and either a composition series for G_1 or a normal series of length n . By induction, they are both composition series and are equivalent. In particular (C) must be a composition series for K_2 , and has length $n - 2$. Now

$$\cdots (C) \cdots K_2 \not\leq H_1 \text{ and } 1 = H_{n'} \not\leq H_{n'-1} \not\leq \cdots \not\leq H_1$$

are, respectively, a composition series for H_1 of length $n - 1$ and a normal series for H_1 of length $n' - 1 \geq n - 1$. Again by induction the second series is a composition series equivalent to the first. Consequently the factors of series (3A) are those of (C) , together with G_1/K_2 and G/G_1 . Likewise the factors of (3C) are those of (C) , together with G/H_1 and H_1/K_2 . By the parallelogram law, we are finished. \square

Alternative proof. Lang uses the “Zassenhaus Butterfly Lemma” to prove the following theorem, from which the uniqueness part of Jordan-Hölder follows immediately.

Schreier Refinement Theorem. *Any two normal (S) -series for a group G have equivalent refinements.*

Proof. Take a normal S -series

$$1 = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G.$$

This “filtration” of G allows us to filter any subgroup and any quotient. Thus if $L \leq G$, then

$$1 = L \cap G_n \triangleleft L \cap G_{n-1} \triangleleft \cdots \triangleleft L \cap G_1 \triangleleft L \cap G_0 = L$$

is a normal series of L , by the second isomorphism theorem applied to the subgroups $H = L \cap G_{i-1}$ and $K = G_i$ of G_{i-1} .

To do an analogous thing with a quotient G/H , given $H \triangleleft G$, we must raise everything “above the level of H ”; remember that the set of subgroups of G/H are in bijective correspondence with the set of subgroups of G containing H . From our normal series for G and the normal subgroup H we get a “partial” normal series (going down only to H)

$$H = G_n H \triangleleft G_{n-1} H \triangleleft \cdots \triangleleft G_1 H \triangleleft G_0 H = G$$

which when reduced modulo H gives a normal series for G/H (with the same factors, up to isomorphism).

Exercise. $G_{i-1}H/G_iH$ is a quotient of G_{i-1}/G_i . (Hint. Apply the parallelogram law to G_{i-1} and G_iH .)

Now if we have $K \triangleleft H \leq G$ (H/K is then called a “section” of G), we can apply both of the above to filter H/K by our given normal series for G . The result is a partial normal series from K to H :

$$K = (H \cap G_n)K \triangleleft (H \cap G_{n-1})K \triangleleft \cdots \triangleleft (H \cap G_1)K \triangleleft (H \cap G_0)K = H.$$

Now we are ready to consider a second given normal series for the same group G :

$$1 = H_m \triangleleft H_{m-1} \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = G.$$

We may apply the filtering process to each H_{i-1}/H_i , thereby refining the normal series of H 's by replacing $H_i \triangleleft H_{i-1}$ by the longer

$$H_i = (H_{i-1} \cap G_n)H_i \triangleleft (H_{i-1} \cap G_{n-1})H_i \triangleleft \cdots \triangleleft (H_{i-1} \cap G_1)H_i \triangleleft (H_{i-1} \cap G_0)H_i = H_{i-1}.$$

We have thus refined the series of H 's to a series of length mn whose factors are

$$(H_{i-1} \cap G_{j-1})H_i / (H_{i-1} \cap G_j)H_i, \quad 1 \leq i \leq m, \quad 1 \leq j \leq n.$$

In the same way we can refine the series of G 's to another series of length mn whose factors are

$$(H_{i-1} \cap G_{j-1})G_j / (H_i \cap G_{j-1})G_j, \quad 1 \leq i \leq m, \quad 1 \leq j \leq n.$$

The proof is completed by the Zassenhaus Butterfly Lemma, which states that the two groups just displayed are isomorphic: \square

Lemma (Zassenhaus). $(H_{i-1} \cap G_{j-1})H_i / (H_{i-1} \cap G_j)H_i \cong (H_{i-1} \cap G_{j-1})G_j / (H_i \cap G_{j-1})G_j$ for all i, j .

Proof. Apply the parallelogram law to $(H_{i-1} \cap G_j)H_i$ and $H_{i-1} \cap G_{j-1}$. Since $H_i \triangleleft H_{i-1}$ and $G_j \triangleleft G_{j-1}$, the first of these is normalized by the second. We first need to simplify the intersection of these two groups:

$$[(H_{i-1} \cap G_j)H_i] \cap (H_{i-1} \cap G_{j-1}) = (H_{i-1} \cap G_j)[H_i \cap (H_{i-1} \cap G_{j-1})] = (H_{i-1} \cap G_j)(H_i \cap G_{j-1}),$$

the first step by the modular law * (as $H_{i-1} \cap G_j \leq H_{i-1} \cap G_{j-1}$) and the second step since $H_i \leq H_{i-1}$. Notice that the resulting expression is symmetric in G 's and H 's, so a similar application of the parallelogram law brings the other group in the statement of the lemma to the same form. \square

* **Modular Law.**

If A, B and C are subgroups of G , and $A \leq C$, then $AB \cap C = A(B \cap C)$.

Proof. Clearly the right side is contained in the left side as $A \leq C$. Conversely if $c \in AB \cap C$, we write $c = ab$, $a \in A$, $b \in B$ and conclude that $b = a^{-1}c \in C$ since $A \leq C$. Thus $b \in B \cap C$ so $c = ab \in A(B \cap C)$.

Corollary. *The dimension of a finite-dimensional vector space is uniquely determined.*

Proof. A basis $\{v_1, \dots, v_n\}$ of the vector space V gives rise to the normal series

$$0 = V_n \subsetneq V_{n-1} \subsetneq \dots \subsetneq V_1 \subsetneq V_0 = V$$

where V_i is the span of v_{i+1}, \dots, v_n . This is in fact a composition series as each factor is the span of a single vector. Now apply U) of Jordan-Hölder. QED

Corollary. *Unique factorization holds in \mathbf{Z} .*

The proof is left to the reader, and is based on the fact that a factorization of n yields a composition series for the cyclic group \mathbf{Z}_n .

Corollary. *Let Γ be any group and ϕ a representation of Γ on the finite-dimensional vector space V . Then V has a filtration by Γ -invariant subspaces*

$$0 = V_n \subsetneq V_{n-1} \subsetneq \dots \subsetneq V_1 \subsetneq V_0$$

such that each V_{i-1}/V_i affords an irreducible representation of Γ . Moreover any two such filtrations are equivalent in the sense of Jordan-Hölder.

The irreducible representations corresponding to the V_{i-1}/V_i are called the irreducible constituents of ϕ .

Problem. *Determine all finite groups by determining a) the simple ones and b) all groups with a given set of composition factors.*

Both these seem impossible, but a) has been solved and b) seems far too complex to leave any hope for a clear solution. However, 30 years ago the same was thought of a) !!

In the remaining parts of this section we address a) by giving some more examples of simple groups, and address b) by discussing solvable groups, which in the finite case are those built from the simplest composition factors—cyclic groups of prime order.

3d. Solvable Groups

The following result is easy:

Proposition. *All subgroups and quotients of an abelian group are abelian.*

However the “converse” is false; if $N \triangleleft G$ and N and G/N are both abelian, then G need not be abelian. Example: $G = \Sigma_3$, $N = A_3$, or $G = D_{2n}$, $N \cong \mathbf{Z}_n$. To obtain a property which “persists under extensions” in the most economical way we are led to the following notion.

Definition. A finite group is solvable if and only if all its composition factors are abelian (hence cyclic of prime order). In general a group is solvable if and only if there exists a normal series (by definition of finite length!) all of whose factors are abelian.

The two definitions coincide for finite groups, since if a finite group has such a normal series then it can be refined to a composition series, whence all composition factors are abelian.

Example: Σ_4 is solvable. For any $v = (ab)(cd) \in V - \{1\}$, the series

$$1 \triangleleft \langle v \rangle \triangleleft V \triangleleft A_4 \triangleleft \Sigma_4$$

is a composition series.

Proposition. All subgroups and quotients of solvable groups are solvable. If $N \triangleleft G$, and both N and G/N are solvable, then G is solvable.

Proof If $K \triangleleft H \leq G$, and $A \leq G$, then $A \cap K \triangleleft A \cap H$ and $A \cap H/A \cap K$ is isomorphic to a subgroup of H/K . This follows from the parallelogram law applied to K and $A \cap H$. Now if

$$1 = G_n \triangleleft_{\neq} G_{n-1} \triangleleft_{\neq} \cdots \triangleleft_{\neq} G_2 \triangleleft_{\neq} G_1 \triangleleft_{\neq} G_0 = G$$

is a normal series of G with abelian factors, then

$$1 = G_n \cap H \triangleleft_{\neq} G_{n-1} \cap H \triangleleft_{\neq} \cdots \triangleleft_{\neq} G_2 \cap H \triangleleft_{\neq} G_1 \cap H \triangleleft_{\neq} G_0 \cap H = H \quad (5A)$$

is a normal series of H , and $G_{i-1} \cap H/G_i \cap H$ embeds in the abelian group G_{i-1}/G_i so is abelian. The statement for quotients similarly follows from the following fact: If $K \triangleleft H \leq G$ and $N \triangleleft G$, then $KN \triangleleft HN$ and HN/KN is isomorphic to a quotient of H/K . The parallelogram law applied to KN and H yields in fact that $HN/KN \cong H/H \cap KN$; but $K \leq H \cap KN$ so $H/H \cap KN$ is a quotient of H/K . In this situation the above series gives the series

$$N = NG_n \triangleleft_{\neq} NG_{n-1} \triangleleft_{\neq} \cdots \triangleleft_{\neq} NG_2 \triangleleft_{\neq} NG_1 \triangleleft_{\neq} NG_0 = G \quad (5B)$$

and so

$$1 = N/N \triangleleft_{\neq} NG_{n-1}/N \triangleleft_{\neq} \cdots \triangleleft_{\neq} NG_2/N \triangleleft_{\neq} NG_1/N \triangleleft_{\neq} NG_0/N = G/N \quad (5C)$$

the factors of which are quotients of the original abelian factors so are again abelian.

Conversely suppose that N and G/N are solvable. Then G/N has a normal series with abelian factors, and replacing each term by its inverse image in G and using the correspondence theorem we get a series starting with N and going to G , with all factors abelian. We are assuming that N possesses such a series, and it can be attached to this one to give the desired series for G .

One useful way to analyze a solvable group is by its action on a minimal normal subgroup.

Theorem. Let G be a finite solvable group. Let $1 \neq N \triangleleft G$ and suppose that no proper subgroup of N is normal in G . Then $N \cong Z_p \times \cdots \times Z_p$ for some prime p .

A group is called elementary abelian if it is the direct product of groups of the same prime order. The structure theorem for finite abelian groups (see below) implies that if N is a finite abelian group and p a prime such that $x^p = 1$ for all $x \in N$, then N is elementary abelian. We shall use this fact in the proof, and aim to prove that N is abelian and has exponent p .

The proof uses the notion of characteristic subgroup:

Definition. A subgroup $H \leq G$ is characteristic in G if and only if $\alpha(H) = H$ for all $\alpha \in \text{Aut}(G)$. We write $H \text{ char } G$.

If $H \text{ char } G$, then $\text{Int}(g)(H) = H$ for all $g \in G$, so $gHg^{-1} = H$, i.e., $H \triangleleft G$. The converse is false.

It also uses the notion of commutator subgroup.

Definition. Let $x, y \in G$. Then $[x, y] = xyx^{-1}y^{-1}$. Moreover, $[G, G] = \langle [x, y] \mid x, y \in G \rangle$.

A group is abelian if and only if $[G, G] = 1$.

Lemma. The following subgroups of any group G are characteristic subgroups:

- a) $[G, G]$;
- b) $Z(G)$;
- c) $G^n = \langle x^n \mid x \in G \rangle$, for an integer n .

Moreover, if G is finite and has a normal Sylow p -subgroup P for some prime p , then $P \text{ char } G$.

Proof ${}^g[x, y] = [{}^gx, {}^gy]$ so conjugation by an element of G leaves the set of commutators invariant; therefore it leaves invariant the subgroup generated by them. The proof for c) is similar, and b) is left to the reader. For the final statement, P is the only Sylow p -subgroup, being normal, so is characteristic since automorphisms carry Sylow p -subgroups to Sylow p -subgroups. QED

Lemma. If $H \text{ char } N \triangleleft G$, then $H \triangleleft G$.

Proof Let $g \in G$. Then $\text{Int}(g) : x \mapsto gxg^{-1}$ is an automorphism of G , and it leaves N invariant since $N \triangleleft G$. Therefore $\text{Int}(g)|_N$ is an automorphism of N , so it leaves the characteristic subgroup H invariant. Therefore $gHg^{-1} = H$. QED

Here is the universal property of $[G, G]$, or really the quotient $G/[G, G]$, or really the projection $G \rightarrow [G, G]$.

Proposition. If $N \leq G$, then $N \geq [G, G]$ if and only if $N \triangleleft G$ and G/N is abelian.

Proof Suppose $[G, G] \leq N \leq G$. Then for any $g \in G$ and $n \in N$, $gnng^{-1} = [g, n]n \in N$, so $N \triangleleft G$. Now under the projection $G \rightarrow G/N$, $[x, y]$ maps to $[xN, yN]$. But $[x, y] = 1$ for all x, y since $[G, G] \leq N$. Therefore $[G/N, G/N] = 1$. Conversely if N is a normal subgroup and G/N is abelian, the same reasoning shows that $[x, y] \in N$ for all $x, y \in G$. Therefore $[G, G] \leq N$.

Corollary. $[G, G] < G$ if and only if G has a nontrivial abelian quotient. If G is a solvable group and $G \neq 1$, then $[G, G] < G$.

Proof of Theorem Let G and N be as in the theorem. Then N is solvable since G is solvable. So $[N, N] < N$. But $[N, N] \text{ char } N \triangleleft G$ so $[N, N] \triangleleft G$. Therefore $[N, N] = 1$ and N is abelian. Let p be a prime divisor of $|N|$. The mapping $N \rightarrow N$ defined by $x \mapsto x^p$ is then a homomorphism, with image N^p . Its kernel is nontrivial by Sylow, and so $N^p < N$. As with the commutator subgroup we get $N^p = 1$, that is, $x^p = 1$ for all $x \in N$. Now we quote the structure theorem for finite abelian groups (see below) to complete the proof.

3e. More Simple Groups

So far the simple groups which we have encountered are all finite: \mathbf{Z}_p for p prime, and A_n for $n \geq 5$.

Exercise. Let Ω be an infinite set and let Σ_Ω^o be the subgroup of Σ_Ω consisting of all elements with finite support, i.e. all g such that $g\omega = \omega$ for all but finitely many $\omega \in \Omega$. Define A_Ω^o in a natural way, and prove that A_Ω^o is simple. (Hint. Let $N \triangleleft A_\Omega^o$. Prove and use the fact that for any finite subset $\Psi \subseteq \Omega$, $N \cap A_\Psi = 1$ or A_Ψ , where A_Ψ is considered as a subgroup of A_Ω^o in the obvious way.)

Another source for simple groups, finite or infinite, is matrix groups, i.e. certain subgroups and quotients (and subgroups of quotients) of $GL_n(K)$ for various fields K . We define

$$PGL_n(K) = GL_n(K)/Z \text{ and } PSL_n(K) = SL_n(K)/Z \cap SL_n(K)$$

where Z is the group of all scalar matrices (scalar multiples of the identity matrix) in $GL_n(K)$. Notice that $Z \leq Z(GL_n(K))$.

Exercise. $Z = Z(GL_n(K))$.

Also by the parallelogram law, $PSL_n(K) \cong ZSL_n(K)/Z \triangleleft PGL_n(K)$. So $PGL_n(K)$ has a copy of $PSL_n(K)$ as a normal subgroup.

Theorem. Let K be a field and $n \geq 2$ an integer. If $n = 2$ assume that $|K| \geq 4$. Then $PSL_2(K)$ is simple.

The “P” in PGL and PSL is for “projective”. Another source for simple groups are matrix groups, i.e. certain subgroups and quotients (and subgroups of quotients) of $GL_n(K)$ for various fields K . We define

$$PGL_n(K) = GL_n(K)/Z \text{ and } PSL_n(K) = SL_n(K)/Z \cap SL_n(K)$$

where Z is the group of all scalar matrices (scalar multiples of the identity matrix) in $GL_n(K)$. Notice that $Z \leq Z(GL_n(K))$.

Exercise. $Z = Z(GL_n(K))$.

Also by the parallelogram law, $PSL_n(K) \cong ZSL_n(K)/Z \triangleleft PGL_n(K)$. So $PGL_n(K)$ has a copy of $PSL_n(K)$ as a normal subgroup.

Theorem. *Let K be a field and $n \geq 2$ an integer. If $n = 2$ assume that $|K| \geq 4$. Then $PSL_2(K)$ is simple.*

The “ P ” in PGL and PSL is for “projective”.

We sketch a proof. Let V be a 2-dimensional vector space over the field K . Define $GL(V)$ to be the group of nonsingular linear transformations: $V \rightarrow V$; $SL(V)$ to be the subgroup of $GL(V)$ which is the kernel of the determinant homomorphism $GL(V) \rightarrow K^\times$; Z to be the subgroup of $GL(V)$ consisting of all scalar mappings (for each $\alpha \in K^\times$ there is unique corresponding scalar mapping $s_\alpha \in GL(V)$, namely $s_\alpha(v) = \alpha v$ for all $v \in V$). Also define $PGL(V) = GL(V)/Z$ and $PSL(V) = SL(V)/Z \cap SL(V)$.

Choosing a (ordered) basis for V leads to an isomorphism $PSL(V) \cong PSL_2(K)$. We may then think of $PSL(V)$ acting on $\mathbf{P}(V)$, or equivalently, we may think of $PSL_2(K)$ acting on the set of 1-dimensional spaces of 2×1 column vectors.

The group $GL(V)$ acts naturally on the set $\mathbf{P}(V)$ of 1-dimensional subspaces of V , so $SL(V)$ does as well. Moreover Z acts trivially on $\mathbf{P}(V)$, so the action $GL(V) \rightarrow \Sigma_{\mathbf{P}(V)}$ lifts to an action $GL(V)/Z \rightarrow \Sigma_{\mathbf{P}(V)}$, i.e., $PGL(V)$ acts on $\mathbf{P}(V)$. Likewise $PSL(V)$ acts on $\mathbf{P}(V)$.

Exercise. *The action of $PSL(V)$ on $\mathbf{P}(V)$ is 2-transitive.*

We also can show:

Lemma. *The action of $PSL(V)$ on $\mathbf{P}(V)$ is faithful.*

This amounts to showing that if $T : V \rightarrow V$ is a linear transformation and for each $v \in V$ there exists a scalar α_v (depending on v , perhaps) such that $Tv = \alpha_v v$, then $\alpha_v = \alpha_w$ for all $v, w \in V - \{0\}$. (Look at $T(v + w)$ to see that this is true, if v and w are linearly independent.)

The structure of a point stabilizer is also important, and this is easily seen concretely in $PSL_2(K)$.

Lemma. *The stabilizer in $PSL_2(K)$ of the subspace ω spanned by $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is the image \overline{B} in $PSL_2(K)$ of the group*

$$B = \left\{ \begin{bmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{bmatrix} \mid \alpha \in K^\times, \beta \in K \right\}.$$

under the canonical homomorphism $SL_2(K) \rightarrow PSL_2(K)$. (B is a subgroup of $SL_2(K)$; check it.)

This merely states that

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \zeta \\ 0 \end{bmatrix}$$

for some ζ if and only if $\gamma = 0$.

Lemma. B and \overline{B} are solvable.

Proof. Define $\phi : B \rightarrow K^\times$ by

$$\phi \left(\begin{bmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{bmatrix} \right) = \alpha.$$

It is easily checked that ϕ is a homomorphism. Let $u(\beta) = \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}$ for any $\beta \in K$, and

$$U = \ker \phi = \{u(\beta) \mid \beta \in K\}.$$

Then U is abelian and B/U is isomorphic to a subgroup of K^\times so is abelian. Therefore the normal series $B > U > 1$ has abelian factors and so B is solvable. Since \overline{B} is the image of B , it is isomorphic to a quotient of B and so is solvable.

We need one additional fact about $PSL_2(K)$; to motivate it we now give the main logic of the proof.

Main Logic Let $G = PSL_2(K)$, which acts on $\Omega = \mathbf{P}(V)$. Suppose that $N \triangleleft G$, but $1 < N < G$. We derive a contradiction.

Since G acts faithfully and 2-transitively on Ω , and $N \neq 1$, N is transitive on Ω (the same fact was used in the proof that A_n is simple, $n \geq 5$). Therefore $G = NG_\omega = \overline{B}N$. (For any $g \in G$ there is $n \in N$ with $g\omega = n\omega$ and so $g = gn^{-1}n \in G_\omega N$. Then $G/N = \overline{B}N/N \cong \overline{B}/\overline{B} \cap N$ is a quotient of the solvable group \overline{B} so is solvable. Since $N \neq G$, G/N is a nontrivial (solvable) group. Therefore it has a nontrivial abelian quotient. Therefore G has a nontrivial abelian quotient. Therefore $SL_2(K)$ has a nontrivial abelian quotient. Therefore $SL_2(K) \neq [SL_2(K), SL_2(K)]$. This completes the proof as it contradicts the following fact:

Lemma. If $|K| \geq 4$, and $H = SL_2(K)$, then $H = [H, H]$.

The lemma is proved by

- a) checking that $H = SL_2(K)$ is generated by all the elements $u(\beta)$ defined above and all their transposes $v(\beta) = u(\beta)^T$. (This amounts to showing that any matrix of determinant 1 can be reduced to I by certain types of row and column operations.)

- b) checking that each $u(\beta)$ and $v(\beta)$ lies in $[H, H]$. (It is here that the hypothesis $|K| \geq 4$ is used, to find an element $\alpha \in K$ such that $\alpha \neq 0$ and $\alpha \neq \pm 1$. Fix α and let $h(\alpha)$ be the diagonal matrix with diagonal entries α, α^{-1} ; one computes

$$[h(\alpha), u(\beta)] = u((\alpha^2 - 1)\beta).$$

As β varies over K , so does $(\alpha^2 - 1)\beta$, since $\alpha^2 \neq 1$. Therefore every $u(\beta)$ is in $[H, H]$, and similarly so is every $v(\beta)$.

Then as the u 's and v 's generate H , $[H, H] = H$. \square

A similar argument, slightly more complicated, can be used to prove:

Theorem. *For any field K and any $n \geq 3$, $PSL_n(K)$ is simple.*

There are no exceptions here; the larger size of matrices makes it possible to express certain critical matrices as commutators, regardless of the size of the field.