

Math 551 – Algebra – Fall 2000

Richard Lyons
Rutgers University
New Brunswick, New Jersey, USA

A. Groups

3. The Meat-Axe: Homomorphisms and Noether Isomorphism Theorems.

One fundamental principle of “modern” algebra which we have assiduously ignored until now is that in studying structures, the real idea of “structure” is contained not in the definition of what kinds of objects are to be studied (e.g. groups) but rather in the definition of what mappings between the objects will be studied (e.g. group homomorphisms). Anything invariant under all these mappings is considered part of the “structure”.

In any case, it is almost heretical for us to have come this far without defining the notion of group homomorphism. Somehow we have scraped by with just “isomorphism”. Furthermore, from a practical point of view it is hardly possible to continue without this notion. It is not a matter of religion but of experience that benefits steadily accrue from thinking in terms of mappings and not just objects. For example, the fact that two groups are isomorphic is often less to the point than the fact that a certain mapping is an isomorphism.

3a. Homomorphisms and normal subgroups

Definition. Let G and H be groups. A homomorphism $\phi : G \rightarrow H$ is a mapping such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$.

The following are then immediate consequences of the definition.

- 1) An isomorphism is a bijective homomorphism.
- 2) The composite of two homomorphisms is a homomorphism.
- 3) If $\phi : G \rightarrow H$ is a homomorphism then
 - a) $\phi(1_G) = 1_H$,
 - b) $\phi(x_1 \cdots x_n) = \phi(x_1) \cdots \phi(x_n)$ for all $x_1, \dots, x_n \in G$, and
 - c) $\phi(x^m) = (\phi(x))^m$, for all $x \in G$ and all integers m (including negative integers, and $m = -1$ in particular).
- 4) If $\phi : G \rightarrow H$ is a homomorphism, then any equation or collection of equations which holds in G is transformed by ϕ to a true equation or collection of equations in H .

- 5) If $\phi : G \rightarrow H$ is a homomorphism and $K \leq G$, then $\phi(K) \leq H$. In particular $\phi(G) \leq H$.
- 6) If $H \leq G$, then the inclusion mapping $H \rightarrow G$ is a homomorphism.

The following example of a homomorphism is important. Let the group G act on the set Ω . Define

$$\lambda : G \rightarrow \Sigma_\Omega \text{ by } \lambda(g)(\alpha) = g\alpha.$$

The axiom $g(h\alpha) = (gh)\alpha$ translates to $\lambda(gh) = \lambda(g)\lambda(h)$, while $1\alpha = \alpha$ translates to $\lambda(1) = 1$. These imply that $\lambda(g^{-1})$ is an inverse to $\lambda(g)$, so each $\lambda(g)$ does indeed lie in Σ_Ω .

In fact a group action of G on Ω is equivalent to a homomorphism $G \rightarrow \Sigma_\Omega$. Just turn around the above discussion; given a homomorphism λ , define $g\alpha = \lambda(g)(\alpha)$ and check the two axioms for group action, which are equivalent to the two properties of homomorphisms as above.

As a nontrivial example of such a homomorphism, let $G = \Sigma_4$. Of course G acts on $\{1, 2, 3, 4\}$ in the obvious way. Let Ω be the set of partitions of $\{1, 2, 3, 4\}$ into two subsets of cardinality 2. Thus one element of Ω is the partition $\pi = \{\{1, 2\}, \{3, 4\}\}$. There are just three elements of Ω . Moreover G acts on Ω in the natural way, e.g. $g\pi = \{\{g1, g2\}, \{g3, g4\}\}$. Thus we obtain a homomorphism

$$\phi_{4,3} : \Sigma_4 \rightarrow \Sigma_\Omega \cong \Sigma_3.$$

There are three fundamental types of homomorphisms, and any homomorphism is a composite of one of each type (the first isomorphism theorem): a projection onto a quotient group, followed by an isomorphism, followed by an inclusion mapping of a subgroup, namely $\phi(G)$ into H . The only nontrivial one of these three is the first, which we now discuss.

Definition. If $K \leq G$, then K is a normal subgroup of G if and only if ${}^gK = K$ for all $g \in G$. We write $K \triangleleft G$.

Examples. $1 \triangleleft G$ and $G \triangleleft G$ always. In an abelian group, every subgroup is a normal subgroup. In D_{2n} , $n > 2$, the rotation subgroup (of index 2) is a normal subgroup, but the group generated by a single reflection is not a normal subgroup.

Notice that the condition $K \triangleleft G$, i.e. $gKg^{-1} = K$ for all $g \in G$, is equivalent to: $gK = Kg$, for every $g \in G$, that is, the left cosets of K in G are also right cosets (and vice-versa).

Moreover, to check that $K \triangleleft G$, it suffices to check that $gKg^{-1} \subseteq K$ for all $g \in G$. For then for any $g \in G$ we have

$$gKg^{-1} \subseteq K \text{ and } g^{-1}K(g^{-1})^{-1} \subseteq K;$$

the latter implies that $gKg^{-1} \supseteq K$ and so $gKg^{-1} = K$.

Definition. If $\phi : G \rightarrow H$ is a homomorphism, then the kernel of ϕ is

$$\ker(\phi) = \phi^{-1}(1) = \{g \in G \mid \phi(g) = 1\}.$$

Example. Consider $\phi_{4,3}$, defined as above from Σ_4 to Σ_3 . For each $\alpha \in \Omega$ there is a permutation $\sigma_\alpha \in \Sigma_4$ of order 2 which leaves each of the two subsets comprising α invariant, and within each subset interchanges its two elements. It is easy to check that $\sigma_\alpha \in \ker(\phi_{4,3})$. Indeed if we set

$$V = \{\sigma_\alpha \mid \alpha \in \Omega\} \cup \{1\},$$

the “Klein four-group” or “Viergruppe”, then V is easily checked to be a subgroup of G which is abelian of order 4 and exponent 2, and

$$\ker(\phi_{4,3}) = V.$$

The inclusion \supseteq has been remarked above. To obtain the equality, first check that $\phi_{4,3}$ is surjective, and then count, using the following fact.

Proposition. If $\phi : G \rightarrow H$ is a homomorphism, then $\ker(\phi) \triangleleft G$. Moreover the fibers of ϕ are the (left=right) cosets of $\ker(\phi)$ in G . Finally ϕ is injective if and only if $\ker(\phi) = 1$.

Proof. Let $K = \ker \phi$. If $x \in K$ and $g \in G$ then $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(1)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(1) = 1$. Hence $gKg^{-1} \subseteq K$. As g was arbitrary, $K \triangleleft G$.

Next, fix $x \in G$. Then the fiber over $\phi(x)$ contains the element $y \in G$ if and only if $\phi(y) = \phi(x) \iff \phi(y)\phi(x)^{-1} = 1 \iff \phi(yx^{-1}) = 1 \iff yx^{-1} \in K \iff y \in Kx$. So the fibers of ϕ are the right cosets of K in G . In particular, as ϕ is injective if and only if all these fibers are singletons, ϕ is injective if and only if $|K| = 1$, which is equivalent to $K = 1$. QED

A corollary of this proposition is that if G is finite and $\phi : G \rightarrow H$ is a homomorphism, then $|G|/|\ker(\phi)| = |\phi(G)|$. (A more precise statement will be proved below as the first isomorphism theorem.) In particular in the example above, $24 = |\Sigma_4| = |\ker(\phi_{4,3})||\Sigma_3| = 6|\ker(\phi_{4,3})|$ (as $\phi_{4,3}$ is surjective). Therefore $|\ker(\phi_{4,3})| = 4$ and so $\ker(\phi_{4,3}) = V$.

3b. Quotients

Let G be a group and $K \triangleleft G$. In this special situation G/K inherits a group structure from G , namely

$$(gK) \cdot (g'K) = (gg')K.$$

The normality of K is needed to check that this is well defined. In fact if we use the following natural definition of multiplication of subsets of G :

$$XY = \{xy \mid x \in X, y \in Y\}, \tag{*}$$

then

$$(gK)(g'K) = g(Kg')K = g(g'K)K = (gg')KK = (gg')K = (gK) \cdot (g'K)$$

which proves that the operation \cdot on G/K is well-defined. Moreover it is clear from (*) and the associative law in G that $(XY)Z = X(YZ)$ for all subsets X, Y, Z of G , so the operation \cdot is associative. The coset K is an identity element: $gK \cdot K = K \cdot gK = gK$, and for any $gK \in G/K$, the coset $g^{-1}K$ is an inverse for gK . Therefore G/K is a group, **and** the mapping

$$\pi_K : G \rightarrow G/K \text{ taking } g \mapsto gK$$

is a homomorphism, called the (canonical) projection of G on G/K .

The key point about G/K and π_K , rather than the cooked-up definition of G/K as a set of cosets, is the fact that π_K is a homomorphism whose kernel is precisely K : Every normal subgroup is the kernel of some homomorphism.

One may think of G/K as consisting of elements \bar{g} , as g varies over G ; but it is possible for \bar{g} to equal \bar{h} even if g and h are different in G . In fact the equations $\bar{g} = \bar{1}$ for all $g \in K$ are imposed in G/K , and all consequences of these equations and the group axioms must therefore also hold. The fact that the kernel of the canonical projection π_K is just K means that the equations $\bar{g} = \bar{1}$, $g \in K$ do not imply any further equation of the form $\bar{g} = \bar{1}$ for some $g \in G - K$. But of course they do imply that $\bar{g} = \bar{g}'$ whenever $g \in g'K$.

3c. The Noether Isomorphism Theorems

Now we can prove the three fundamental isomorphism theorems 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.

QED

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

Example. The mapping $\phi : SL_2(\mathbf{C}) \rightarrow PSL_2(\mathbf{C})$ defined earlier, taking

$$\phi : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto F_{a,b,c,d}$$

where $F_{a,b,c,d}$ is the Möbius transformation

$$z \mapsto \frac{az + b}{cz + d}$$

of the complex plane, is a homomorphism (i.e. the composite of Möbius transformations gets its coefficients from the two factors the same way the product of matrices does). Moreover the kernel of ϕ is

$$\ker \phi = \langle -I \rangle = \{I, -I\}$$

i.e., the only ways to represent the identity transformation as a Möbius transformation with $ad - bc = 1$ are as $z = 1 \cdot z/1$ or $z = (-1) \cdot z/(-1)$.

Moreover ϕ is surjective and so the first isomorphism theorem gives

$$PSL_2(\mathbf{C}) \cong SL_2(\mathbf{C})/\langle -I \rangle.$$

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 $T, T' \in \mathcal{T}$:
 - a) $S \leq S'$ if and only if $\phi(S) \leq \phi(S')$, and if these conditions hold then $|S' : S| = |\phi(S') : \phi(S)|$;
 - b) $S \triangleleft S'$ if and only if $\phi(S) \triangleleft \phi(S')$, and if these conditions hold then $S'/S \cong \phi(S')/\phi(S)$;
 - c) $\phi(S \cap S') = \phi(S) \cap \phi(S')$.
 - d) $\phi(\langle S, S' \rangle) = \langle \phi(S), \phi(S') \rangle$.

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 $G/H / K/H \cong G/K$.

Corollary. *Suppose that there exists a surjective homomorphism $\phi : G \rightarrow H$ of groups. Let $N \triangleleft G$. Then there exists a surjective homomorphism $G/N \rightarrow H/\phi(N)$.*

The proofs are left to the reader.

3d. Groups with operators

The preceding discussion of homomorphisms and Noether isomorphisms 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 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 ${}^g(\phi(h)) = \phi({}^g h)$ 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

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

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.

3e. 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.

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 G_1 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:

$$1 \not\triangleleft K \not\triangleleft H \not\triangleleft G \text{ or } 1 \not\triangleleft H \not\triangleleft K \not\triangleleft G.$$

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

$$1 = G_n \not\triangleleft G_{n-1} \not\triangleleft \cdots \not\triangleleft G_2 \not\triangleleft G_1 \not\triangleleft G_0 = 1 \quad (3A)$$

in which

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

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 :

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

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

$$1 \not\triangleleft G_{n-1} \not\triangleleft \cdots \not\triangleleft G_2 \not\triangleleft G_1 \not\triangleleft G,$$

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

$$1 = H_{n'} \not\triangleleft H_{n'-1} \not\triangleleft \cdots \not\triangleleft H_2 \not\triangleleft H_1 \not\triangleleft H_0 = G, \quad (3C)$$

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

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

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

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

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

is a normal series of L , because of the following lemma:

Lemma. *If $K \triangleleft H \leq G$ and $L \leq G$, then $K \cap L \triangleleft H \cap L$. Moreover $H \cap L / K \cap L$ is isomorphic to a subgroup of H/K .*

Proof. Apply the parallelogram law to K and $H \cap L$, which normalizes K . We get $H \cap L \cap K \triangleleft H \cap L$, giving the first statement since $K \leq H$ so that $H \cap L \cap K = L \cap K$. Moreover

$$H \cap L / K \cap L \cong (H \cap L)K / K \leq L / K.$$

\square

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

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

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

Exercise. $G_{i-1}K/G_iK$ is a quotient of G_{i-1}/G_i .

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) !!