

Math 551 – Algebra – Fall 2000

Richard Lyons
Rutgers University
New Brunswick, New Jersey, USA

A. Groups

5. The Analysis of Groups.

We consider here the question of how properties of a group G may be related to properties of its normal subgroups N and quotients G/N . We also give some natural ways to attempt to break up a group into simpler parts. We also give some examples of simple groups.

5a. Some Simple Groups

Of course the cyclic groups \mathbf{Z}_p of prime order are simple, and they are the only simple abelian groups (If G is simple abelian then every subgroup is normal, so is either 1 or G , so $G = \langle g \rangle$ for any $1 \neq g \in G$. Let p be a prime divisor of $|G|$ (or any prime if G is infinite). Then $\langle g^p \rangle < G$ so $g^p = 1$.)

One classic family of nonabelian simple groups is the family of alternating groups.

Theorem. *Suppose that $n \geq 5$. Then A_n is simple.*

Corollary. *Suppose that $n \geq 5$. Then the only nontrivial normal subgroup of Σ_n is A_n .*

A standard approach to proving this theorem is a) show that A_n is generated by all its 3-cycles (note that we can't use 2-cycles since they are odd permutations); b) show that all 3-cycles in A_n are conjugate in A_n ; c) show that if $1 < N \triangleleft A_n$, then an element of N whose support has minimum size is a 3-cycle. Then by c) and b), N contains all 3-cycles, so equals G , as desired. The dirtiest part of this is c), where one produces from an element $g \in A_n$ which is not a 3-cycle another non-identity element $h \in A_n$ which has smaller support, but is the product of powers of g and their conjugates.

Instead we give an inductive proof, still using the action of A_n on $\Omega = \{1, \dots, n\}$ of course. This is a transitive action for which the stabilizer of a point is isomorphic to A_{n-1} .

To start the induction, observe that A_5 has 15 “Klein” elements (those of shape $(ab)(cd)e$), and they are all conjugate in A_5 . A_5 also has 20 3-cycles, and they too are all conjugate in A_5 . A_5 has 24 5-cycles, each of which is self-centralizing and so lies in a conjugacy class of size $|A_5|/5 = 12$. The class equation for A_5 is therefore

$$60 = 1 + 15 + 20 + 12 + 12.$$

Now a normal subgroup N of A_5 must consist of the identity and some of the other conjugacy classes, so $|N|$ is a subsum of the above sum, containing the term 1. But no such subsum divides 60, other than the full sum or 1. Therefore $N = 1$ or $N = A_5$.

For the induction step, we need to check that for $n \geq 6$, the action of A_n on $\{1, \dots, n\}$ is 4-transitive in the following sense.

Definition. Let G act on Ω . Then G acts 4-transitively if and only if for any quadruple $(\alpha, \beta, \gamma, \delta) \in \Omega \times \Omega \times \Omega \times \Omega$ such that $\alpha, \beta, \gamma, \delta$ are pairwise distinct, and for any other such quadruple $(\alpha', \beta', \gamma', \delta')$, there is $g \in G$ such that $g\alpha = \alpha'$, $g\beta = \beta'$, $g\gamma = \gamma'$, and $g\delta = \delta'$.

One may similarly define n -transitivity, using n -tuples instead of quadruples.

Lemma. If G acts n -transitively on Ω , then for each $\omega \in \Omega$, G_ω acts $n - 1$ -transitively on $\Omega - \{\omega\}$.

Proof Left to reader.

Lemma. For $n \geq 6$, A_n acts 4-transitively on $\{1, \dots, n\}$.

Proof Σ_n certainly does, and if g is taken in Σ_n and is odd, then $g' = g\tau$ works just as well, where τ is a transposition fixing $\alpha, \beta, \gamma, \delta$.

A group action of G on Ω is called faithful if and only if the kernel of the corresponding mapping $G \rightarrow \Sigma_\Omega$ is trivial. The action of A_n on $\{1, \dots, n\}$ is certainly faithful.

Lemma. Suppose that G acts n -transitively and faithfully on Ω , $n \geq 2$. Let $1 \neq N \triangleleft G$. Then N acts transitively on Ω . Moreover, if $N_\alpha = 1$ for some $\alpha \in \Omega$, then the action of G on $N - \{1\}$ by conjugation is $n - 1$ -transitive.

Proof For any $\omega \in \Omega$, the N -orbit $N \cdot \omega$ is mapped by $g \in G$ as follows:

$$g \cdot (N \cdot \omega) = (gN) \cdot \omega = Ng \cdot \omega = N(g\omega)$$

Thus each $g \in G$ permutes the set of N -orbits on Ω . Suppose that there are two or more orbits $\Omega_1, \Omega_2, \dots$. Then $|\Omega_i| > 1$ since otherwise N would act trivially on Ω , so $N = 1$ by faithfulness, contrary to assumption. Choose $\alpha, \beta \in \Omega_1$ and $\gamma \in \Omega_2$. There is $g \in G$ such that $g\alpha = \alpha$ and $g\beta = \gamma$. Therefore $g\Omega_1 = \Omega_1$ and $g\Omega_1 = \Omega_2$, a contradiction. Therefore there's only one orbit and N is transitive.

Next fix $\alpha \in \Omega$ and suppose that $N_\alpha = 1$. We map

$$\phi : N \rightarrow \Omega, n \mapsto n\alpha,$$

and claim that ϕ is a bijection. Since N is transitive ϕ is onto. If $n\alpha = n'\alpha$ then $n^{-1}n' \in N_\alpha = 1$ so $n = n'$. We also claim that

the actions of G_α on N (by conjugation) and Ω are isomorphic via ϕ ,

that is, $\phi(gn) = g\phi(n)$ for all $g \in G_\alpha$ and $n \in N$. Namely, $\phi(gn) = \phi(gng^{-1}) = gng^{-1}\alpha = gn\alpha = g\phi(n)$.

But the action of G_α on $\Omega - \{\alpha\}$ is $n - 1$ -transitive, and so its action on $N - \{1\}$ is $n - 1$ -transitive as well. \square

Now we complete the proof of the theorem. Suppose that $n \geq 6$ and let $G = A_n$. Proceeding by contradiction suppose that $N \triangleleft G$, with $N \neq 1$ and $N \neq G$. We reach a contradiction. Let $\alpha \in \{1, \dots, n\} = \Omega$. Then $G_\alpha \cap N \triangleleft G_\alpha$ by the parallelogram law. But $G_\alpha \cong A_{n-1}$ is simple by induction. Therefore $G_\alpha \cap N = G_\alpha$ or 1 . Also N is transitive on Ω , so $|N : N_\alpha| = n$.

If $G_\alpha \cap N = 1$, then $N_\alpha = 1$ and so $|N| = n$. The previous lemma shows that G_α acts $4 - 1$ -transitively on $N - \{1\}$ by conjugation, since G is 4 -transitive on Ω . Choose distinct elements $x, y \in N - \{1\}$ and let $z = xy$, so that z is distinct from x and y . As $n \geq 6$ there is another element $w \in N - \{1\}$. By the 3 -transitivity of G_α there is $g \in G_\alpha$ such that

$$gxg^{-1} = x, \quad gyg^{-1} = y, \quad gzg^{-1} = w.$$

However, $gzg^{-1} = gxg^{-1}gyg^{-1} = xy = z \neq w$, a contradiction.

Therefore $G_\alpha \cap N = G_\alpha$ so $G_\alpha = N_\alpha$. Then $|G : G_\alpha| = n = |N : N_\alpha| = |N : G_\alpha|$ and so $N = G$. \square

Proof of Corollary. Suppose that $n \geq 5$ and $N \triangleleft \Sigma_n$. Then $N \cap A_n \triangleleft A_n$ so $N \cap A_n = 1$ or A_n . In the first case $N \cong N/N \cap A_n \leq \Sigma_n/A_n \cong Z_2$, so $|N| \leq 2$. If $|N| = 2$, then N consists of a single odd element which must be the unique element of its cycle shape (as $N \triangleleft G$). But clearly for each cycle shape (except for the identity element) there is more than one element of that cycle shape, contradiction. In the second case $A_n \leq N$ and the Correspondence Theorem implies $N = A_n$ or Σ_n .

5b. 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 are both abelian, then G need not be abelian. Example: $G = \Sigma_3$, $N = A_3$, or $G = D_{2n}$, $N \cong Z_n$. 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 $v \in V - \{1\}$, 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

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

is a normal series of G with abelian factors, then

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

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

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

and so

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

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 $n \in N$, $gng^{-1} = [g, n]n \in N$, 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.

5c. N/C -Theorem

The fact that a solvable group has a normal subgroup which is elementary abelian suggests a way to analyze the group: consider the series

$$1 \leq N \leq C_G(N) \leq G.$$

Here the centralizer of a subgroup N is defined as

$$C_G(N) = \{g \in G \mid gn = ng \forall n \in N\}.$$

It is easily checked that $C_G(N)$ is a subgroup of G . It is not always true that $N \leq C_G(N)$; indeed this condition is equivalent to N being abelian.

Thus we have the three factors N , $C_G(N)$ and $G/C_G(N)$. Of these we have little control over $C_G(N)$, but since $N \triangleleft G$, $G/C_G(N)$ can be regarded as a subgroup of $\text{Aut}(N)$ as follows.

Theorem. *Let $N \triangleleft G$. The mapping $G \rightarrow \text{Aut}(N)$ defined by $g \mapsto \text{Int}(g)|_N$ is a homomorphism, and its kernel is $C_G(N)$. Consequently $C_G(N) \triangleleft G$ and $G/C_G(N)$ is isomorphic to a subgroup of $\text{Aut}(N)$.*

The assertions of the theorem are easy to check and are left to the reader.

When N is not necessarily normal, we salvage at least this much:

Corollary. *Let $H \leq G$. Then the mapping $N_G(H) \rightarrow \text{Aut}(H)$ defined by $g \mapsto \text{Int}(g)|_H$ is a homomorphism with kernel $C_G(H)$. Consequently $C_G(H) \triangleleft N_G(H)$ and $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.*

Furthermore,

5d. More Simple Groups

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”. 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 $\Omega = \mathbf{P}(\mathbf{V})$. 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 $\overline{g} = gn^{-1}n \in G_\omega N$. 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 , $[H, H] = H$. ◻

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.

5e. Inner and Outer Automorphisms

This is one of the “natural ways” referred to above. For any group G , and any $g \in G$, the mapping

$$\text{Int}(g) : G \rightarrow G, h \mapsto ghg^{-1}$$

is an automorphism of G . Any automorphism of G arising from some element $g \in G$ in this fashion is called an inner automorphism of G . Furthermore, the mapping

$$I : G \rightarrow \text{Aut}(G), g \mapsto \text{Int}(g)$$

is then a homomorphism: $\text{Int}(gg') = \text{Int}(g)\text{Int}(g')$. (Check it!) The

image of I consists of all inner automorphisms, which therefore constitute a subgroup $\text{Inn}(G) \leq \text{Aut}(G)$.

Theorem. $\ker I = Z(G)$, and $G/Z(G) \cong \text{Inn}(G) \triangleleft \text{Aut}(G)$.

Proof $z \in \ker I \iff zgz^{-1} = g$ for all $g \in G \iff z \in Z(G)$. The first isomorphism theorem then gives the isomorphism. The normality of $\text{Inn}(G)$ follows from the following identity:

$$\text{If } \alpha \in \text{Aut}(G) \text{ and } g \in G, \text{ then } \alpha \text{Int}(g)\alpha^{-1} = \text{Int}(\alpha(g)).$$

Namely $\alpha \text{Int}(g)\alpha^{-1}(h) = \alpha(g\alpha^{-1}(h)g^{-1}) = \alpha(g)h\alpha(g)^{-1}$.

Elements of $\text{Aut}(G)/\text{Inn}(G) \cong \text{Out}(G)$ are called “outer automorphisms”. The following conjecture is a consequence of the classification of finite simple groups, but still awaits a straightforward proof.

Schreier Conjecture. *If G is a finite simple group, then $\text{Out}(G)$ is solvable.*

Not every group can arise as $\text{Inn}(G)$ for some G . For instance:

Theorem. *If $G/Z(G)$ is cyclic, then G is abelian (and so $G/Z(G) = 1$).*

Proof. Some element $gZ(G) \in G/Z(G)$ generated $G/Z(G)$. Then $G = \cup g^i Z(G)$. Consequently $G = \langle S \rangle$ where $S = Z(G) \cup \{g\}$. But any two elements of S commute, hence any two elements of G commute, since they are represented by words in S .

Corollary. *If $|G| = p^2$ for some prime p , then $G \cong \mathbf{Z}_p \times \mathbf{Z}_p$ or \mathbf{Z}_{p^2} .*

Proof. Since $|G| = p^2$ we know that $Z(G) \neq 1$. Therefore $G/Z(G)$ has order 1 or p , so is cyclic. By the theorem, G is abelian. If G has an element of order p^2 , then $G \cong \mathbf{Z}_{p^2}$. Otherwise every element of G has order p (except the identity element). Choose $g \in G$ with $g \neq 1$, so $\langle g \rangle \cong \mathbf{Z}_p$. Then $\langle g \rangle \neq G$ and we may choose $h \in G$ with $h \notin \langle g \rangle$. Construct the abstract group $\langle g \rangle \times \langle h \rangle$ and define

$$\phi : \langle g \rangle \times \langle h \rangle \rightarrow G$$

by $\phi((g^i, h^j)) = g^i h^j$. Since G is abelian this turns out to be a homomorphism. Its image clearly contains both $\langle g \rangle$ and $\langle h \rangle$ so by Lagrange's Theorem its image is all of G . Since $|\langle g \rangle \times \langle h \rangle| = p^2 = |G|$ and ϕ is surjective, ϕ must be an isomorphism. QED