GROUP THEORY

J.S. MILNE

August 21, 1996; v2.01

Abstract. Thes are the notes for the first part of Math 594, University of Michigan, Winter 1994, exactly as they were handed out during the course except for some minor corrections.

Please send comments and corrections to me at jmilne@umich.edu using "Math594" as the subject.

Contents

References:

Dummit and Foote, Abstract Algebra.
Rotman, An Introduction to the Theory of Groups

1. Basic Definitions

1.1. Definitions.

Definition 1.1. A is a nonempty set G together with a law of composition $(a, b) \mapsto a * b : G \times G \to G$ satisfying the following axioms:

(a) (associative law) for all $a, b, c \in G$,

$$(a * b) * c = a * (b * c);$$

(b) (existence of an identity element) there exists an element $e \in G$ such that $a * e = a = e * a$ for all $a \in G$;

(c) (existence of inverses) for each $a \in G$, there exists an $a' \in G$ such that

$$a * a' = e = a' * a.$$

If (a) and (b) hold, but not necessarily (c), then G is called a *semigroup.* (Some authors don't require a semigroup to contain an identity element.)

We usually write $a * b$ and e as ab and 1, or as $a + b$ and 0.

Two groups G and G' are *isomorphic* if there exists a one-to-one correspondence $a \leftrightarrow a'$, $G \leftrightarrow G'$, such that $(ab)' = a'b'$ for all $a, b \in G$.

Remark 1.2. In the following, $a, b, \ldots$ are elements of a group G.

(a) If $aa = a$, then $a = e$ (multiply by a'). Thus e is the unique element of G with the property that $ee = e$.

(b) If $ba = e$ and $ac = e$, then

$$b = be = b(ac) = (ba)c = ec = c.$$

Hence the element a' in (1.1c) is uniquely determined by a. We call it the *inverse* of a, and denote it a^{-1} (or the *negative* of a, and denote it $-a$).

(c) Note that (1.1a) allows us to write $a_1a_2a_3$ without bothering to insert parentheses. The same is true for any finite sequence of elements of G. For definiteness, define

$$a_1a_2 \cdots a_n = (\cdots((a_1a_2)a_3)a_4 \cdots).$$

Then an induction argument shows that the value is the same, no matter how the parentheses are inserted. (See Dummit p20.) Thus, for any finite *ordered* set S of elements in G, $\prod_{a \in S} a$ is defined. For the empty set S, we set it equal to 1.

(d) The inverse of $a_1a_2 \cdots a_n$ is $a_n^{-1}a_{n-1}^{-1} \cdots a_1^{-1}$.

(e) Axiom (1.1c) implies that cancellation holds in groups:

$$ab = ac \implies b = c, \qquad ba = ca \implies b = c$$

(multiply on left or right by a^{-1}). Conversely, if G *is finite*, then the cancellation laws imply Axiom (c): the map $x \mapsto ax : G \to G$ is injective, and hence (by counting) bijective; in particular, 1 is in the image, and so a has a right inverse; similarly, it has a left inverse, and we noted in (b) above that the two inverses must then be equal.

The *order* of a group is the number of elements in the group. A finite group whose order is a power of a prime p is called a *p-group.*[1]

[1] Throughout the course, p will always be a prime number.

Define

$$a^n = \begin{cases} aa\cdots a & n > 0 \quad (n \text{ copies}) \\ 1 & n = 0 \\ a^{-1}a^{-1}\cdots a^{-1} & n < 0 \quad (n \text{ copies}) \end{cases}$$

The usual rules hold:

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}. \tag{1.1}$$

It follows from (1.1) that the set

$$\{n \in \mathbb{Z} \mid a^n = 1\}$$

is an ideal in $\mathbb{Z}$. Therefore, this set equals (m) for some $m \geq 0$. If $m = 0$, then a is said to have *infinite order*, and $a^n \neq 1$ unless $n = 0$. Otherwise, a is said to have *finite order* m, and m is the smallest positive integer such that $a^m = 1$. In this case, $a^n = 1 \iff m|n$; moreover $a^{-1} = a^{m-1}$.

Example 1.3. (a) For each $m = 1, 2, 3, 4, \ldots, \infty$ there is a cyclic group of order m, C_m. When $m < \infty$, then there is an element $a \in G$ such that

$$G = \{1, a, \ldots, a^{m-1}\},$$

and G can be thought of as the group of rotations of a regular polygon with n-sides. If $m = \infty$, then there is an element $a \in G$ such that

$$G = \{a^m \mid m \in \mathbb{Z}\}.$$

In both cases $C_m \approx \mathbb{Z}/m\mathbb{Z}$, and a is called a generator of C_m.

(b) Probably the most important groups are matrix groups. For example, let R be a commutative ring[2]. If X is an $n \times n$ matrix with coefficients in R whose determinant is a unit in R, then the cofactor formula for the inverse of a matrix (Dummit p365) shows that X^{-1} also has coefficients[3] in R. In more detail, if X' is the transpose of the matrix of cofactors of X, then $X \cdot X' = \det X \cdot I$, and so $(\det X)^{-1}X'$ is the inverse of X. It follows that the set $\mathrm{GL}_n(R)$ of such matrices is a group. For example $\mathrm{GL}_n(\mathbb{Z})$ is the group of all $n \times n$ matrices with integer coefficients and determinant ± 1.

(c) If G and H are groups, then we can construct a new group $G \times H$, called the *product* of G and H. As a set, it is the Cartesian product of G and H, and multiplication is defined by:

$$(g, h)(g', h') = (gg', hh').$$

(d) A group is *commutative* (or *abelian*) if

$$ab = ba, \quad \text{all } a, b \in G.$$

Recall from Math 593 the following classification of finite abelian groups. Every finite abelian group is a product of cyclic groups. If $\gcd(m, n) = 1$, then $C_m \times C_n$ contains an element of order mn, and so $C_m \times C_n \approx C_{mn}$, and isomorphisms of this type give the only ambiguities in the decomposition of a group into a product of cyclic groups.

From this one finds that every finite abelian group is isomorphic to exactly one group of the following form:

$$C_{n_1} \times \cdots \times C_{n_r}, \quad n_1|n_2, \ldots, n_{r-1}|n_r.$$

[2] This means, in particular, that R has an identity element 1. Homomorphisms of rings are required to take 1 to 1.

[3] This also follows from the Cayley-Hamilton theorem.

The order of this group is $n_1 \cdots n_r$.

Alternatively, every abelian group of finite order m is a product of p-groups, where p ranges over the primes dividing m,

$$G \approx \prod_{p|m} G_p.$$

For each partition

$$n = n_1 + \cdots + n_s, \quad n_i \geq 1,$$

of n, there is a group $\prod C_{p^{n_i}}$ of order p^n, and every group of order p^n is isomorphic to exactly one group of this form.

(e) *Permutation groups.* Let S be a set and let G the set $\mathrm{Sym}(S)$ of bijections $\alpha : S \to S$. Then G becomes a group with the composition law $\alpha\beta = \alpha \circ \beta$. For example, the *permutation group on n letters* is $S_n = \mathrm{Sym}(\{1, ..., n\})$, which has order $n!$. The symbol $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 4 & 3 & 1 & 6 \end{smallmatrix}\right)$ denotes the permutation sending $1 \mapsto 2$, $2 \mapsto 5$, $3 \mapsto 7$, etc..

1.2. Subgroups.

Proposition 1.4. *Let G be a group and let S be a nonempty subset of G such that*

(a) $a, b \in S \implies ab \in S$.
(b) $a \in S \implies a^{-1} \in S$.

Then the law of composition on G makes S into a group.

Proof. Condition (a) implies that the law of composition on G does define a law of composition $S \times S \to S$ on S. By assumption S contains at least one element a, its inverse a^{-1}, and the product $e = aa^{-1}$. Finally (b) shows that inverses exist in S. □

A subset S as in the proposition is called a *subgroup* of G.

If S is finite, then condition (a) implies (b): for any $a \in S$, the map $x \mapsto ax : S \to S$ is injective, and hence (by counting) bijective; in particular, 1 is in the image, and this implies that $a^{-1} \in S$. The example $\mathbb{N} \subset \mathbb{Z}$ (additive groups) shows that (a) does not imply (b) when G is infinite.

Proposition 1.5. *An intersection of subgroups of G is a subgroup of G.*

Proof. It is nonempty because it contains 1, and conditions (a) and (b) of the definition are obvious. □

Remark 1.6. It is generally true that an intersection of sub-algebraic-objects is a subobject. For example, an intersection of subrings is a subring, an intersection of submodules is a submodule, and so on.

Proposition 1.7. *For any subset X of a group G, there is a smallest subgroup of G containing X. It consists of all finite products (allowing repetitions) of elements of X and their inverses.*

Proof. The intersection S of all subgroups of G containing X is again a subgroup containing X, and it is evidently the smallest such group. Clearly S contains with X, all finite products of elements of X and their inverses. But the set of such products satisfies (a) and (b) of (1.4) and hence is a subgroup containing X. It therefore equals S. □

We write $<X>$ for the subgroup S in the proposition, and call it the *subgroup generated* by X. For example, $<\emptyset>=\{1\}$. If every element of G has finite order, for example, if G is finite, then the set of all finite products of elements of X is already a group (recall that if $a^m=1$, then $a^{-1}=a^{m-1}$) and so equals $<X>$.

We say that X *generates* G if $G=<X>$, i.e., if every element of G can be written as a finite product of elements from X and their inverses.

A group is *cyclic* if it is generated by one element, i.e., if $G=<a>$. If a has finite order m, then

$$G=\{1,a,a^2,...,a^{m-1}\}\approx\mathbb{Z}/m\mathbb{Z},\quad a^i\leftrightarrow i \mod m.$$

If a has infinite order, then

$$G=\{\dots,a^{-i},\dots,a^{-1},1,a,\dots,a^i,\dots\}\approx\mathbb{Z},\quad a^i\leftrightarrow i.$$

Note that the order of an element a of a group is the order of the subgroup $<a>$ it generates.

1.3. Groups of order <16.

Example 1.8. (a) *Dihedral group*, D_n. This is the group of symmetries of a regular polygon with n-sides. Let σ be the rotation through $2\pi/n$, and let τ be a rotation about an axis of symmetry. Then

$$\sigma^n=1;\quad \tau^2=1;\quad \tau\sigma\tau^{-1}=\sigma^{-1}\quad (\text{or } \tau\sigma=\sigma^{n-1}\tau).$$

The group has order $2n$; in fact

$$D_n=\{1,\sigma,...,\sigma^{n-1},\tau,...,\sigma^{n-1}\tau\}.$$

(b) *Quaternion group* Q : Let $a=\begin{pmatrix}0&\sqrt{-1}\\ \sqrt{-1}&0\end{pmatrix}$, $b=\begin{pmatrix}0&1\\ -1&0\end{pmatrix}$. Then

$$a^4=1,\quad a^2=b^2,\quad bab^{-1}=a^{-1}.$$

The subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by a and b is

$$Q=\{1,a,a^2,a^3,b,ab,a^2b,a^3b\}.$$

The group Q can also be described as the subset $\{\pm1,\pm i,\pm j,\pm k\}$ of the quaternion algebra.

(c) Recall that S_n is the permutation group on $\{1,2,...,n\}$. The *alternating group* is the subgroup of even permutations (see later). It has order $\frac{n!}{2}$.

Every group of order <16 is isomorphic to exactly one on the following list:

1: C_1. 2: C_2. 3: C_3.

4: C_4, $C_2\times C_2$ (Viergruppe; Klein 4-group).

5: C_5.

6: C_6, $S_3=D_3$. (S_3 is the first noncommutative group.)

7: C_7.

8: C_8, $C_2\times C_4$, $C_2\times C_2\times C_2$, Q, D_4.

9: C_9, $C_3\times C_3$.

10: C_{10}, D_5.

11: C_{11}.

12: C_{12}, $C_2\times C_2\times C_3$, $C_2\times S_3$, A_4, $C_3\rtimes C_4$ (see later).

13: C_{13}.

14: C_{14}, D_7.

15: C_{15}.

16: (14 groups)

General rules: For each prime p, there is only one group (up to isomorphism), namely C_p, and only two groups of order p^2, namely, $C_p \times C_p$ and C_{p^2}. (We'll prove this later.) Roughly speaking, the more high powers of primes divide n, the more groups of order n you expect. In fact, if $f(n)$ is the number of isomorphism classes of groups of order n, then

$$f(n) \leq n^{(\frac{2}{27}+o(1))\mu^2} \qquad \text{as } \mu \to \infty$$

where p^μ is the highest prime power dividing n and $o(1) \to 0$ as $\mu \to \infty$ (see Pyber, Ann. of Math., 137 (1993) 203–220).

1.4. Multiplication tables.

A finite group can be described by its multiplication table:

	1	a	b	c	$\ldots$
1	1	a	b	c	$\ldots$
a	a	a^2	ab	ac	$\ldots$
b	b	ba	b^2	bc	$\ldots$
c	c	ca	cb	c^2	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Note that, because we have the cancellation laws in groups, each row (and each column) is a permutation of the elements of the group. Multiplication tables give us an algorithm for classifying all groups of a given finite order, namely, list all possible multiplication tables and check the axioms, but it is not practical! There are n^3 possible multiplication tables for a group of order n, and so this quickly becomes unmanageable. Also checking the associativity law from a multiplication table is very time consuming. Note how few groups there are! Of 12^3 possible multiplication tables for groups of order 12, only 5 actually give groups.

1.5. Homomorphisms.

Definition 1.9. A *homomorphism* from a group G to a second G' is a map $\alpha : G \to G'$ such that $\alpha(ab) = \alpha(a)\alpha(b)$ for all a, b.

Note that an isomorphism is simply a bijective homomorphism.

Remark 1.10. Let α be a homomorphism. By induction, $\alpha(a^m) = \alpha(a)^m$, $m \geq 1$. Moreover $\alpha(1) = \alpha(1 \times 1) = \alpha(1)\alpha(1)$, and so $\alpha(1) = 1$ (see Remark (1.2a). Finally

$$aa^{-1} = 1 = a^{-1}a \implies \alpha(a)\alpha(a^{-1}) = 1 = \alpha(a)\alpha(a)^{-1}.$$

From this it follows that

$$\alpha(a^m) = \alpha(a)^m \qquad \text{all } m \in \mathbb{Z}.$$

We saw above that each row of the multiplication table of a group is a permutation of the elements of the group. As Cayley pointed out, this allows one to realize the group as a group of permutations.

Theorem 1.11 (Cayley's theorem). *There is a canonical injective homomorphism*

$$\alpha : G \hookrightarrow \mathrm{Sym}(G).$$

Proof. For $a \in G$, define $a_L : G \to G$ to be the map $x \mapsto ax$ (left multiplication by a). For $x \in G$,

$$(a_L \circ b_L)(x) = a_L(b_L(x)) = a_L(bx) = abx = (ab)_L(x),$$

and so $(ab)_L = a_L \circ b_L$. In particular,

$$a_L \circ (a^{-1})_L = \mathrm{id} = (a^{-1})_L \circ a_L$$

and so a_L is a bijection, i.e., $a_L \in \mathrm{Sym}(G)$. We have shown that $a \mapsto a_L$ is a homomorphism, and it is injective because of the cancellation law. □

Corollary 1.12. *A finite group of order n can be identified with a subgroup of S_n.*

Proof. Number the elements of the group $a_1, \ldots, a_n$. □

Unfortunately, when G has large order n, S_n is too large to be manageable. We shall see presently that G can often be embedded in a permutation group of much smaller order than $n!$.

1.6. Cosets.

Let H be a subgroup of G. A *left coset* of H in G is a set of the form $aH =_{df} \{ah \mid h \in H\}$, some fixed $a \in G$; a *right coset* is a set of the form $Ha = \{ha \mid h \in H\}$, some fixed $a \in G$.

Example 1.13. Let $G = \mathbb{R}^2$, regarded as a group under addition, and let H be a subspace (line through the origin). Then the cosets (left or right) of H are the lines parallel to H.

It is not difficult to see that the condition "a and b are in the same left coset" is an equivalence relation on G, and so the left cosets form a partition of G, but we need a more precise result.

Proposition 1.14. *(a) If C is a left coset of H, and $a \in C$, then $C = aH$.*

(b) Two left cosets are either disjoint or equal.

(c) $aH = bH$ if and only if $a^{-1}b \in H$.

(d) Any two left cosets have the same number of elements.

Proof. (a) Because C is a left coset, $C = bH$ some $b \in G$. Because $a \in C$, $a = bh$ for some $h \in H$. Now $b = ah^{-1} \in aH$, and for any other element c of C, $c = bh' = ah^{-1}h' \in aH$. Conversely, if $c \in aH$, then $c = ah' = bhh' \in bH$.

(b) If C and C' are not disjoint, then there is an element $a \in C \cap C'$, and $C = aH$ and $C' = aH$.

(c) We have $aH = bH \iff b \in aH \iff b = ah$, for some $h \in H$, i.e., $\iff a^{-1}b \in H$.

(d) The map $(ba^{-1})_L : ah \mapsto bh$ is a bijection $aH \to bH$. □

The *index* $(G : H)$ of H in G is defined to be the number of left cosets of H in G. In particular, $(G : 1)$ is the order of G. The lemma shows that G is a disjoint union of the left cosets of H, and that each has the same number of elements. When G is finite, we can conclude:

Theorem 1.15 (Lagrange). *If G is finite, then $(G:1)=(G:H)(H:1)$. In particular, the order of H divides the order of G.*

Corollary 1.16. *If G has order m, then the order of every element g in G divides m.*

Proof. Apply Lagrange's theorem to $H=<g>$, recalling that $(H:1)=\text{order}(g)$. □

Example 1.17. If G has order p, a prime, then every element of G has order 1 or p. But only e has order 1, and so G is generated by any element $g\neq e$. In particular, G is cyclic, $G\approx C_p$. Hence, up to isomorphism, there is only one group of order 1,000,000,007; in fact there are only two groups of order 1,000,000,014,000,000,049.

Remark 1.18. (a) There is a one-to-one correspondence between the set of left cosets and the set of right cosets, viz, $aH\leftrightarrow Ha^{-1}$. Hence $(G:H)$ is also the number of right cosets of H in G. But, in general, a left coset will not be a right coset (see below).

(b) Lagrange's theorem has a partial converse: if a prime p divides $m=(G:1)$, then G has an element of order p; if p^n divides m, then G has a subgroup of order p^n (Sylow theorem). But note that $C_2\times C_2$ has order 4, but has no element of order 4, and A_4 has order 12, but it has no subgroup of order 6.

More generally, we have the following result (for G finite).

Proposition 1.19. *If $G\supset H\supset K$ with H and K subgroups of G, then*

$$(G:K)=(G:H)(H:K).$$

Proof. Write $G=\bigcup g_iH$ (disjoint union), and $H=\bigcup h_jK$ (disjoint union). On multiplying the second equality by g_i, we find that $g_iH=\bigcup_j g_ih_jK$ (disjoint union), and so $G=\bigcup g_ih_jK$ (disjoint union). □

1.7. Normal subgroups.

If S and T are two subsets of G, then we write $ST=\{st\mid s\in S,\quad t\in T\}$.

A subgroup N of G is *normal*, written $N\lhd G$, if $gNg^{-1}=N$ for all $g\in G$. An intersection of normal subgroups of a group is normal.

Remark 1.20. To show N normal, it suffices to check that $gNg^{-1}\subset N$ for all g : for

$$gNg^{-1}\subset N\implies g^{-1}gNg^{-1}g\subset g^{-1}Ng \text{ (multiply left and right with } g^{-1} \text{ and } g)$$

Hence $N\subset g^{-1}Ng$ for all g. On rewriting this with g^{-1} for g, we find that $N\subset gNg^{-1}$ for all g.

The next example shows however that there can exist an N and a g such that $gNg^{-1}\subset N$, $gNg^{-1}\neq N$ (famous exercise in Herstein).

Example 1.21. Let $G=\mathrm{GL}_2(\mathbb{Q})$, and let $H=\{\left(\begin{smallmatrix}1&n\\0&1\end{smallmatrix}\right)\mid n\in\mathbb{Z}\}$. Then H is a subgroup of G; in fact it is isomorphic to $\mathbb{Z}$. Let $g=\left(\begin{smallmatrix}5&0\\0&1\end{smallmatrix}\right)$. Then

$$g\begin{pmatrix}1&n\\0&1\end{pmatrix}g^{-1}=\begin{pmatrix}5&5n\\0&1\end{pmatrix}\begin{pmatrix}5^{-1}&0\\0&1\end{pmatrix}=\begin{pmatrix}1&5n\\0&1\end{pmatrix}.$$

Hence $gHg^{-1}\subset H$, but $\neq H$.

Proposition 1.22. *A subgroup N of G is normal if and only if each left coset of N in G is also a right coset, in which case, $gN=Ng$ for all $g\in G$.*

Proof. $\Longrightarrow$: Multiply the equality $gNg^{-1} = N$ on the right by g.

$\Longleftarrow$: If gN is a right coset, then it must be the right coset Ng—see (1.14a). Hence $gN = Ng$, and so $gNg^{-1} = N$. This holds for all g. □

Remark 1.23. In other words, in order for N to be normal, we must have that for all $g \in G$ and $n \in N$, there exists an $n' \in N$ such that $gn = n'g$ (equivalently, for all $g \in G$ and $n \in N$, there exists an n' such that $ng = gn'$.) Thus, an element of G can be moved past an element of N at the cost of replacing the element of N by a different element.

Example 1.24. (a) Every subgroup of index two is normal. Indeed, let $g \in G$, $g \notin H$. Then $G = H \cup gH$ (disjoint union). Hence gH is the complement of H in G. The same argument shows that Hg is the complement of H in G. Hence $gH = Hg$.

(b) Consider the dihedral group $D_n = \{1, \sigma, \ldots, \sigma^{n-1}, \tau, \ldots, \sigma^{n-1}\tau\}$. Then $C_n = \{1, \sigma, \ldots, \sigma^{n-1}\}$ has index 2, and hence is normal, but for $n \geq 3$ the subgroup $\{1, \tau\}$ is not normal because $\sigma\tau\sigma^{-1} = \tau\sigma^{n-2} \notin \{1, \tau\}$.

(c) Every subgroup of a commutative group is normal (obviously), but the converse is false: the quaternion group Q is not commutative, but every subgroup is normal.

A group G is said to be *simple* if it has no normal subgroups other than G and $\{1\}$. The Sylow theorems (see later) show that such a group will have lots of subgroups (unless it is a cyclic group of prime order)—they just won't be normal.

Proposition 1.25. *If H and N are subgroups of G and N (or H) is normal, then*

$$HN =_{df} \{hn \mid h \in H, \quad n \in N\}$$

is a subgroup of G. If H is also normal, then HN is a normal subgroup of G.

Proof. It is nonempty, and

$$(hn)(h'n') \overset{1.23}{=} hh'n''n' \in HN,$$

and so it is closed under multiplication. Since

$$(hn)^{-1} = n^{-1}h^{-1} \overset{1.23}{=} h^{-1}n' \in HN$$

it is also closed under the formation of inverses. □

1.8. Quotients.

The *kernel* of a homomorphism $\alpha : G \to G'$ is

$$\mathrm{Ker}(\alpha) = \{g \in G | \ \alpha(g) = 1\}.$$

Proposition 1.26. *The kernel of a homomorphism is a normal subgroup.*

Proof. If $a \in \mathrm{Ker}(\alpha)$, so that $\alpha(a) = 1$, and $g \in G$, then

$$\alpha(gag^{-1}) = \alpha(g)\alpha(a)\alpha(g)^{-1} = \alpha(g)\alpha(g)^{-1} = 1.$$

Hence $gag^{-1} \in \mathrm{Ker}\,\alpha$. □

Proposition 1.27. *Every normal subgroup occurs as the kernel of a homomorphism. More precisely, if N is a normal subgroup of G, then there is a natural group structure on the set of cosets of N in G (this is if and only if).*

Proof. Write the cosets as left cosets, and define $(aN)(bN) = (ab)N$. We have to check (a) that this is well-defined, and (b) that it gives a group structure on the set of cosets. It will then be obvious that the map $g \mapsto gN$ is a homomorphism with kernel N.

Check (a). Suppose $aN = a'N$ and $bN = b'N$; we have to show that $abN = a'b'N$. But we are given that $a = a'n$ and $b = b'n'$ with $n, n' \in N$. Hence $ab = a'nb'n'$. Because of (1.23) there exists an $n'' \in N$ such that $nb' = b'n''$. Hence $ab = a'b'n''n' \in a'b'N$. Therefore abN and $a'b'N$ have a common element, and so must be equal.

The rest of the proof is straightforward: the set is nonempty; the associative law holds; the coset N is an identity element; $a^{-1}N$ is an inverse of aN. (See Dummit p81.) □

When N is a normal subgroup, we write G/N for the set of left (= right) cosets of N in G, regarded as a group. It is called the *quotient* of G by N. The map $a \mapsto aN : G \to G/N$ is a surjective homomorphism with kernel N. It has the following universal property: for any homomorphism $\alpha : G \to G'$ such that $\alpha(N) = 1$, there exists a unique homomorphism $G/N \to G'$ such that the following diagram commutes:

$$\begin{tikzcd}
G \arrow[r, "a\mapsto aN"] \arrow[dr, "\alpha"'] & G/N \arrow[d] \\
 & G'.
\end{tikzcd}$$

Example 1.28. (a) Consider the subgroup $m\mathbb{Z}$ of $\mathbb{Z}$. The quotient group $\mathbb{Z}/m\mathbb{Z}$ is a cyclic group of order m.

(b) Let L be a line through the origin in $\mathbb{R}^2$, i.e., a subspace. Then $\mathbb{R}^2/L$ is isomorphic to $\mathbb{R}$ (because it is a one-dimensional vector space over $\mathbb{R}$).

(c) The quotient $D_n/ < \sigma > \approx \{1, \tau\}$.

2. Free Groups and Presentations

It is frequently useful to describe a group by giving a set of generators for the group and a set of relations for the generators from which every other relation in the group can be deduced. For example, D_n can be described as the group with generators σ, τ and relations

$$\sigma^n = 1, \quad \tau^2 = 1, \quad \tau\sigma\tau\sigma = 1.$$

In this section, we make precise what this means. First we need to define the free group on a set X of generators—this is a group generated by X and with no relations except for those implied by the group axioms. Because inverses cause problems, we first do this for semigroups.

2.1. Free semigroups.

Recall that (for us) a semigroup is a set G with an associative law of composition having an identity element 1. Let $X = \{a, b, c, \dots\}$ be a (possibly infinite) set of symbols. A *word* is a finite sequence of symbols in which repetition is allowed. For example,

$$aa, \quad aabac, \quad b$$

are distinct words. Two words can be multiplied by juxtaposition, for example,

$$aaaa * aabac = aaaaaabac.$$

This defines on the set W of all words an associative law of composition. The empty sequence is allowed, and we denote it by 1. (In the unfortunate case that the symbol 1 is already an element of X, we denote it by a different symbol.) Then 1 serves as an identity element. Write SX for the set of words together with this law of composition. Then SX is a semigroup, called the *free semigroup* on X.

When we identify an element a of X with the word a, X becomes a subset of SX and generates it (i.e., no proper subsemigroup of SX containing X). Moreover, the map $X \to SX$ has the following universal property: for any map (of sets) $X \to S$ from X to a semigroup S, there exists a unique homomorphism[4] $SX \to S$ making the following diagram commute:

$$\begin{tikzcd} X \arrow[r] \arrow[dr] & SX \arrow[d] \\ & S. \end{tikzcd}$$

In fact, the unique extension of $\alpha : X \to S$ takes the values:

$$\alpha(1) = 1_S, \quad \alpha(dba\cdots) = \alpha(d)\alpha(b)\alpha(a)\cdots.$$

2.2. Free groups.

We want to construct a group FX containing X and having the same universal property as SX with "semigroup" replaced by "group". Define X' to be the set consisting of the symbols in X and also one additional symbol, denoted a^{-1}, for each $a \in X$; thus

$$X' = \{a, a^{-1}, b, b^{-1}, \dots\}.$$

[4] A homomorphism $\alpha : S \to S'$ of semigroups is a map such that $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in S$ and $\alpha(1) = 1$, i.e., α preserves all finite products.

Let W' be the set of words using symbols from X'. This becomes a semigroup under juxtaposition, but it is not a group because we can't cancel out the obvious terms in words of the following form:

$$\cdots xx^{-1} \cdots \text{ or } \cdots x^{-1}x \cdots$$

A word is said to be *reduced* if it contains no pairs of the form xx^{-1} or $x^{-1}x$. Starting with a word w, we can perform a finite sequence of cancellations to arrive at a reduced word (possibly empty), which will be called the *reduced form* of w. There may be many different ways of performing the cancellations, for example,

$$cabb^{-1}a^{-1}c^{-1}ca \mapsto caa^{-1}c^{-1}ca \mapsto cc^{-1}ca \mapsto ca$$

$$cabb^{-1}a^{-1}c^{-1}ca \mapsto cabb^{-1}a^{-1}a \mapsto cabb^{-1} \mapsto ca.$$

Note that the middle a^{-1} is cancelled with different a's, and that different terms survive in the two cases. Nevertheless we ended up with the same answer, and the next result says that this always happens.

Proposition 2.1. *There is only one reduced form of a word.*

Proof. We use induction on the length of the word w. If w is reduced, there is nothing to prove. Otherwise a pair of the form xx^{-1} or $x^{-1}x$ occurs—assume the first, since the same argument works in both cases. If we can show that every reduced form of w can be obtained by first cancelling xx^{-1}, then the proposition will follow from the induction hypothesis applied to the (shorter) word obtained by cancelling xx^{-1}.

Observe that the reduced form w_0 obtained by a sequence of cancellations in which xx^{-1} is cancelled at some point is uniquely determined, because the result will not be affected if xx^{-1} is cancelled first.

Now consider a reduced form w_0 obtained by a sequence in which no cancellation cancels xx^{-1} directly. Since xx^{-1} does not remain in w_0, at least one of x or x^{-1} must be cancelled at some point. If the pair itself is not cancelled, then the first cancellation involving the pair must look like

$$\cdots \cancel{x}^{-1}\underline{\cancel{x}x^{-1}} \cdots \text{ or } \cdots \underline{x\ \cancel{x}^{-1}}\ \cancel{x} \cdots$$

where our original pair is underlined. But the word obtained after this cancellation is the same as if our original pair were cancelled, and so we may cancel the original pair instead. Thus we are back in the case proved above. □

We say two words w, w' are *equivalent*, denoted $w \sim w'$, if they have the same reduced form. This is an equivalence relation (obviously).

Proposition 2.2. *Products of equivalent words are equivalent, i.e.,*

$$w \sim w', \quad v \sim v' \implies wv \sim w'v'.$$

Proof. Let w_0 and v_0 be the reduced forms of w and of v. To obtain the reduced form of wv, we can first cancel as much as possible in w and v separately, to obtain w_0v_0 and then continue cancelling. Thus the reduced form of wv is the reduced form of w_0v_0. A similar statement holds for $w'v'$, but (by assumption) the reduced forms of w and v equal the reduced forms of w' and v', and so we obtain the same result in the two cases. □

Let FX be the set of equivalence classes of words. The proposition shows that the law of composition on W' induces a law of composition on FX, which obviously makes it into a semigroup. It also has inverses, because

$$ab\cdots gh\cdot h^{-1}g^{-1}\cdots b^{-1}a^{-1}\sim 1.$$

Thus FX is a group, called the *free group* on X. To review: the elements of FX are represented by words in X'; two words represent the same element of FX if and only if they have the same reduced forms; multiplication is defined by juxtaposition; the empty word (or aa^{-1} ...) represents 1; inverses are obtained in the obvious way.

When we identify $a\in X$ with the equivalence class of the (reduced) word a, then X becomes identified with a subset of FX—clearly it generates X. The next proposition is a precise expression of the fact that there are no relations among the elements of X when regarded as elements of FX except those imposed by the group axioms.

Proposition 2.3. *For any map (of sets) $X\to G$ from X to a group G, there exists a unique homomorphism $FX\to G$ making the following diagram commute:*

$$\begin{tikzcd} X \arrow[r] \arrow[dr] & FX \arrow[d] \\ & G. \end{tikzcd}$$

Proof. Consider a map $\alpha : X\to G$. We extend it to a map of sets $X'\to G$ by setting $\alpha(a^{-1})=\alpha(a)^{-1}$. Because G is, in particular, a semigroup, α extends to a homomorphism of semigroups $SX'\to G$. This map will send equivalent words to the same element of G, and so will factor through $FX =_{df} S(X)/{\sim}$. The resulting map $FX\to G$ is a group homomorphism. It is unique because we know it on a set of generators for FX. □

Remark 2.4. The universal property of the map $\iota : X\to FX$ characterizes it: if $\iota' : X\to F'$ is a second map with the same property, then there is a unique isomorphism $\alpha : F\to F'$ such that $\alpha(\iota x)=\iota' x$ for all $x\in X$.

Corollary 2.5. *Every group is the quotient of a free group.*

Proof. Choose a set X of generators for G (e.g, $X=G$), and let F be the free group generated by X. Then the inclusion $X\hookrightarrow G$ extends to a homomorphism $F\to G$, and the image, being a subgroup containing X, must be G. □

The free group on the set $X=\{a\}$ is simply the infinite cyclic group C_∞ generated by a, but the free group on a set consisting of two elements is already very complicated. I now discuss, without proof, some important results on free groups.

Theorem 2.6 (Nielsen-Schreier). [5] *Subgroups of free groups are free.*

The best proof uses topology, and in particular covering spaces—see Serre, *Trees*, Springer, 1980, or Rotman, Theorem 12.24.

[5] Nielsen (1921) proved this for finitely generated subgroups, and in fact gave an algorithm for deciding whether a word lies in the subgroup; Schreier (1927) proved the general case.

Two free groups FX and FY are isomorphic if and only if X and Y have the same number of elements[6]. Thus we can define the *rank* of a free group G to be the number of elements in (i.e., cardinality of) a free generating set, i.e., subset $X \subset G$ such that the homomorphism $FX \to G$ given by (2.3) is an isomorphism. Let H be a finitely generated subgroup of a free group F. Then there is an algorithm for constructing from any finite set of generators for H a free finite set of generators. If F has rank n and $(F : H) = i < \infty$, then H is free of rank

$$ni - i + 1.$$

In particular, H may have rank greater than that of F. For proofs, see Rotman, Chapter 12, and Hall, *The Theory of Groups,* Chapter 7.

2.3. Generators and relations.

As we noted in §1.7, an intersection of normal subgroups is again a normal subgroup. Therefore, just as for subgroups, we can define the *normal subgroup generated* by the a set S in a group G to be the intersection of the normal subgroups containing S. Its description in terms of S is a little complicated. Call a subset S of a group G *normal* if $gSg^{-1} \subset S$ for all $g \in G$. Then it is easy to show:

(a) if S is normal, then the subgroup $<S>$ generated[7] by it is normal;
(b) for $S \subset G$, $\bigcup_{g\in G} gSg^{-1}$ is normal, and it is the smallest normal set containing S.

From these observations, it follows that:

Lemma 2.7. *The normal subgroup generated by* $S \subset G$ *is* $<\bigcup_{g\in G} gSg^{-1}>$.

Consider a set X and a set R of words made up of symbols in X'. Each element of R represents an element of the free group FX, and the quotient G of FX by the normal subgroup generated by R is said to have X as *generators* and R as *relations.* One also says that (X, R) is a *presentation* for G, $G =<X|R>$, and that R is a set of *defining relations* for G.

Example 2.8. (a) The dihedral group D_n has generators σ, τ and defining relations $\sigma^n, \tau^2, \tau\sigma\tau\sigma$. (See below for a proof.)

(b) The *generalized quaternion group* Q_n, $n \geq 3$, has generators a, b and relations[8] $a^{2^{n-1}} = 1$, $a^{2^{n-2}} = b^2$, $bab^{-1} = a^{-1}$. For $n = 3$ this is the group Q of (1.8b). In general, it has order 2^n (for more on it, see Ex. 8).

(c) Two elements a and b in a group commute if and only if their *commutator* $[a, b] =_{df} aba^{-1}b^{-1}$ is 1. The free *abelian* group on generators $a_1, \ldots, a_n$ has generators $a_1, a_2, \ldots, a_n$ and relations

$$[a_i, a_j], \qquad i \neq j.$$

(d) The fundamental group of the open disk with one point removed is the free group on σ, a loop around the point. (See Math 591.)

(e) The fundamental group of the sphere with r points removed has generators $\sigma_1, ..., \sigma_r$ (σ_i is a loop around the i^{th} point) and a single relation

$$\sigma_1 \cdots \sigma_r = 1.$$

[6] By which I mean that there is a bijection from one to the other.

[7] Use that conjugation by g, $x \mapsto gxg^{-1}$, is a homomorphism $G \to G$.

[8] Strictly speaking, I should say the relations $a^{2^{n-1}}$, $a^{2^{n-2}}b^{-2}$, $bab^{-1}a$.

(f) The fundamental group of a compact Riemann surface of genus g has 2g generators $u_1, v_1, ..., u_g, v_g$ and a single relation

$$u_1v_1u_1^{-1}v_1^{-1}\cdots u_gv_gu_g^{-1}v_g^{-1}=1.$$

See Massey, *Algebraic Topology:An Introduction,* which contains a good account of the interplay between group theory and topology. For example, for many types of spaces, there is an algorithm for obtaining a presentation for the fundamental group.

Proposition 2.9. *Let G be the group defined by the presentation $\{X, R\}$. For any map (of sets) $X \to H$ from X to a group H each element of R to 1 (in an obvious sense), there exists a unique homomorphism $G \to H$ making the following diagram commute:*

$$\begin{tikzcd} X \arrow[r] \arrow[dr] & G \arrow[d] \\ & H. \end{tikzcd}$$

Proof. Let α be a map $X \to H$. From the universal property of free groups (2.3), we know that α extends to a homomorphism $FX \to H$, which we again denote α. By assumption $R \subset \mathrm{Ker}(\alpha)$, and therefore the normal subgroup N generated by R is contained in $\mathrm{Ker}(\alpha)$. Hence (see p9), α factors through $FX/N = G$. The uniqueness follows from the fact that we know the map on a set of generators for X. □

Example 2.10. Let $G =<a, b|a^n, b^2, baba>$. We prove that G is isomorphic to D_n. Because the elements $\sigma, \tau \in D_n$ satisfy these relations, the map $\{a, b\} \to D_n$, $a \mapsto \sigma$, $b \mapsto \tau$ extends uniquely to a homomorphism $G \to D_n$. This homomorphism is surjective because σ and τ generate D_n. The relations $a^n = 1$, $b^2 = 1$, $ba = a^{n-1}b$ ensure that each element of G is represented by one of the following elements, $1, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b$, and so $(G : 1) \leq 2n = (D_n : 1)$. Therefore the homomorphism is bijective (and these symbols represent distinct elements of G).

2.4. Finitely presented groups.

A group is said to be *finitely presented* if it admits a presentation (X, R) with both X and R finite.

Example 2.11. Consider a finite group G. Let $X = G$, and let R be the set of words

$$\{abc^{-1} \mid ab = c \text{ in } G\}.$$

I claim that (X, R) is a presentation of G, and so G is finitely presented. Let $G' =< X|R>$. The map $FX \to G$, $a \mapsto a$, sends the elements of R to 1, and therefore defines a homomophism $G' \to G$, which is obviously surjective. But note that every element of G' is represented by an element of X, and so the map is an bijective.

Although it is easy to define a group by a finite presentation, calculating the properties of the group can be very difficult—note that we are defining the group, which may be quite small, as the quotient of a huge free group by a huge subgroup. I list some negative results.

The word problem. Let G be the group defined by a finite presentation (X, R). The word problem for G asks whether there is an algorithm (decision procedure) for deciding whether a word on X' represents 1 in G. Unfortunately, the answer is negative: Novikov and Boone showed that there exist finitely presented groups G for which there is no such algorithm. Of course, there do exist other groups for which there is an algorithm.

The same ideas lead to the following result: there does not exist an algorithm that will determine for an arbitary finite presentation whether or not the corresponding group is trivial, finite, abelian, solvable, nilpotent, simple, torsion, torsion-free, free, or has a solvable word problem.

See Rotman, Chapter 13, for proofs of these statements.

The Burnside problem. A group is said to have *exponent m* if $g^m = 1$ for all $g \in G$. It is easy to write down examples of infinite groups generated by a finite number of elements of finite order (see Exercise 2), but does there exist an infinite finitely-generated group with a finite exponent? (Burnside problem). In 1970, Adjan, Novikov, and Britton showed the answer is yes: there do exist infinite finitely-generated groups of finite exponent.

Todd-Coxeter algorithm. There are some quite innocuous looking finite presentations that are known to define quite small groups, but for which this is very difficult to prove. The standard approach to these questions is to use the Todd-Coxeter algorithm (M. Artin, Algebra, p223).

In the remainder of this course, including the exercises, we'll develop various methods for recognizing groups from their presentations.

Maple. What follows is an annotated transcript of a Maple session:

```
maple    [This starts Maple on a Sun, PC, ....]

with(group);    [This loads the group package, and lists some of
the available commands.]

G:=grelgroup({a,b},{[a,a,a,a],[b,b],[b,a,b,a]});
[This defines G to be the group with generators a,b and relations
aaaa, bb, and baba; use 1/a for the inverse of a.]

grouporder(G);      [This attempts to find the order of the group G.]

H:=subgrel({x=[a,a],y=[b]},G);   [This defines H to be the subgroup of
G with generators x=aa and y=b]

pres(H);    [This computes a presentation of H]

quit  [This exits Maple.]
To get help on a command, type ?command
```

3. Isomorphism Theorems; Extensions.

3.1. Theorems concerning homomorphisms.

The next three theorems (or special cases of them) are often called the *first, second, and third isomorphism theorems* respectively.

Factorization of homomorphisms. Recall that, for a homomorphism $\alpha : G \to G'$, the kernel of α is $\{g \in G \mid \alpha(g) = 1\}$ and the image of α is $\alpha(G) = \{\alpha(g) \mid g \in G\}$.

Theorem 3.1 (fundamental theorem of group homomorphisms). *For any homomorphism $\alpha : G \to G'$ of groups, the kernel N of α is a normal subgroup of G, the image I of α is a subgroup of G', and α factors in a natural way into the composite of a surjection, an isomorphism, and an injection:*

$$\begin{tikzcd}
G \arrow[r, "\alpha"] \arrow[d, "onto"] & G' \\
G/N \arrow[r, "\approx"] & I \arrow[u, "inj."']
\end{tikzcd}$$

Proof. We have already seen (1.26) that the kernel is a normal subgroup of G. If $b = \alpha(a)$ and $b' = \alpha(a')$, then $bb' = \alpha(aa')$ and $b^{-1} = \alpha(a^{-1})$, and so $I =_{\mathit{df}} \alpha(G)$ is a subgroup of G'. For $n \in N$, $\alpha(gn) = \alpha(g)\alpha(n) = \alpha(g)$, and so α is constant on each left coset gN of N in G. It therefore defines a map

$$\bar{\alpha} : G/N \to I, \quad \bar{\alpha}(gN) = \alpha(g),$$

which is obviously a homomorphism, and, in fact, obviously an isomorphism. □

The isomorphism theorem.

Theorem 3.2 (Isomorphism Theorem). *Let H be a subgroup of G and N a normal subgroup of G. Then HN is a subgroup of G, $H \cap N$ is a normal subgroup of H, and the map*

$$h(H \cap N) \mapsto hN : H/H \cap N \to HN/N$$

is an isomorphism.

Proof. We have already shown (1.25) that HN is a subgroup. Consider the map

$$H \to G/N, \quad h \mapsto hN.$$

This is a homomorphism, and its kernel is $H \cap N$, which is therefore normal in H. According to Theorem 3.1, it induces an isomorphism $H/H \cap N \to I$ where I is its image. But I is the set of cosets of the form hN, i.e., $I = HN/N$. □

The correspondence theorem. The next theorem shows that if $\bar{G}$ is a quotient group of G, then the lattice of subgroups in $\bar{G}$ captures the structure of the lattice of subgroups of G lying over the kernel of $G \to \bar{G}$. [[Picture.]]

Theorem 3.3 (Correspondence Theorem). *Let $\pi : G \twoheadrightarrow \bar{G}$ be a surjective homomorphism, and let $N = \mathrm{Ker}(\alpha)$. Then there is a one-to-one correspondence*

$$\{\textit{subgroups of } G \textit{ containing } N\} \overset{1:1}{\leftrightarrow} \{\textit{subgroups of } \bar{G}\}$$

under which $H \subset G$ corresponds to $\bar{H} = \alpha(H)$ and $\bar{H} \subset \bar{G}$ corresponds to $H = \alpha^{-1}(\bar{H})$. Moreover, if $H \leftrightarrow \bar{H}$, then

(a) $\bar{H} \subset \bar{H}' \iff H \subset H'$, *in which case* $(\bar{H}' : \bar{H}) = (H' : H)$;
(b) $\bar{H}$ *is normal in* $\bar{G}$ *if and only if* H *is normal in* G, *in which case,* α *induces an isomorphism*
$$G/H \to \bar{G}/\bar{H}.$$

Proof. For any subgroup $\bar{H}$ of $\bar{G}$, $\alpha^{-1}(\bar{H})$ is a subgroup of G containing N, and for any subgroup H of G, $\alpha(H)$ is a subgroup of $\bar{G}$. One verifies easily that $\alpha^{-1}\alpha(H) = H$ if and only if $H \supset N$, and that $\alpha\alpha^{-1}(\bar{H}) = \bar{H}$. Therefore, the two operations give the required bijection. The remaining statements are easily verified. □

Corollary 3.4. *Let N be a normal subgroup of G; then there is a one-to-one correspondence between the subgroups of G containing N and the subgroups of G/N, $H \leftrightarrow H/N$. Moreover H is normal in G if and only if H/N is normal in G/N, in which case the homomorphism $g \mapsto gN : G \to G/N$ induces an isomorphism*
$$G/H \xrightarrow{\approx} (G/N)/(H/N).$$

Proof. Special case of the theorem in which π is taken to be $g \mapsto gN : G \to G/N$. □

3.2. Products. The next two propositions give criteria for a group to be a product of two subgroups.

Proposition 3.5. *Consider subgroups H_1 and H_2 of a group G. The map $(h_1, h_2) \mapsto h_1h_2 : H_1 \times H_2 \to G$ is an isomorphism of groups if and only if*

(a) $G = H_1H_2$,
(b) $H_1 \cap H_2 = \{1\}$, *and*
(c) *every element of H_1 commutes with every element of H_2.*

Proof. The conditions are obviously necessary (if $g \in H_1 \cap H_2$, then $(g, g^{-1}) \mapsto 1$). Conversely, (c) implies that the map $(h_1, h_2) \mapsto h_1h_2$ is a homomorphism, and (b) implies that it is injective:
$$h_1h_2 = 1 \implies h_1 = h_2^{-1} \in H_1 \cap H_2 = \{1\}.$$
Finally, (a) implies that it is surjective. □

Proposition 3.6. *Consider subgroups H_1 and H_2 of a group G. The map $(h_1, h_2) \mapsto h_1h_2 : H_1 \times H_2 \to G$ is an isomorphism of groups if and only if*

(a) $H_1H_2 = G$,
(b) $H_1 \cap H_2 = \{1\}$, *and*
(c) *H_1 and H_2 are both normal in G.*

Proof. Again, the conditions are obviously necessary. In order to show that they are sufficient, we check that they imply the conditions of the previous proposition. For this we only have to show that each element h_1 of H_1 commutes with each element h_2 of H_2. But the commutator $[h_1, h_2] = h_1h_2h_1^{-1}h_2^{-1} = (h_1h_2h_1^{-1}) \cdot h_2^{-1}$ is in H_2 because H_2 is normal, and it's in H_1 because H_1 is normal, and so (b) implies that it is 1. But $[h_1, h_2] = 1$ implies $h_1h_2 = h_2h_1$. □

Proposition 3.7. *Consider subgroups $H_1, H_2, \ldots, H_k$ of a group G. The map*

$$(h_1, h_2, \ldots, h_k) \mapsto h_1h_2 \cdots h_k : H_1 \times H_2 \times \cdots \times H_k \to G$$

is an isomorphism of groups if (and only if)

(a) *each of $H_1, H_2, \ldots, H_k$ is normal in G,*
(b) *for each j, $H_j \cap (H_1 \cdots H_{j-1}H_j \cdots H_k) = \{1\}$, and*
(c) *$G = H_1H_2 \cdots H_k$.*

Proof. For $k = 2$, this is becomes the preceding proposition. We proceed by induction. This allows us to assume that

$$(h_1, h_2, \ldots, h_{k-1}) \mapsto h_1h_2 \cdots h_{k-1} : H_1 \times H_2 \times \cdots \times H_{k-1} \to H_1H_2 \cdots H_{k-1}$$

is an isomorphism. An induction argument using (1.25) shows that $H_1 \cdots H_{k-1}$ is normal in G, and so the pair $H_1 \cdots H_{k-1}$, H_k satisfies the hypotheses of (3.6). Hence

$$(h, h_k) \mapsto hh_k : (H_1 \cdots H_{k-1}) \times H_k \to G$$

is an isomorphism. These isomorphisms can be combined to give the required isomorphism:

$$H_1 \times \cdots \times H_{k-1} \times H_k \xrightarrow{(h_1,\ldots,h_k)\mapsto(h_1\cdots h_{k-1},h_k)} H_1 \cdots H_{k-1} \times H_k \xrightarrow{(h,h_k)\mapsto hh_k} G.$$

□

Remark 3.8. When

$$(h_1, h_2, ..., h_k) \mapsto h_1h_2 \cdots h_k : H_1 \times H_2 \times \cdots \times H_k \to G$$

is an isomorphism we say that G is the direct product of its subgroups H_i. In more down-to-earth terms, this means: each element g of G can be written uniquely in the form $g = h_1h_2 \cdots h_k$, $h_i \in H_i$; if $g = h_1h_2 \cdots h_k$ and $g' = h_1'h_2' \cdots h_k'$, then

$$gg' = (h_1h_1')(h_2h_2') \cdots (h_kh_k').$$

3.3. Automorphisms of groups.

Let G be a group. An isomorphism $G \to G$ is called an *automorphism* of G. The set $\mathrm{Aut}(G)$ of such automorphisms becomes a group under composition: the composite of two automorphisms is again an automorphism; composition of maps is always associative; the identity map $g \mapsto g$ is an identity element; an automorphism is a bijection, and therefore has an inverse, which is again an automorphism.

For $g \in G$, the map i_g "conjugation by g",

$$x \mapsto gxg^{-1} : G \to G$$

is an automorphism: it is a homomorphism because

$$g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}), \quad \text{i.e.,} \quad i_g(xy) = i_g(x)i_g(y),$$

and it is bijective because conjugation by g^{-1} is an inverse. An automorphism of this form is called an *inner automorphism*, and the remaining automorphisms are said to be *outer*.

Note that

$$(gh)x(gh)^{-1} = g(hxh^{-1})g^{-1}, \text{ i.e., } i_{gh}(x) = i_g \circ i_h(x),$$

and so the map $g \mapsto i_g : G \to \operatorname{Aut}(G)$ is a homomorphism. Its image is written $\operatorname{Inn}(G)$. Its kernel is the *centre* of G,

$$Z(G) =_{df} \{g \in G \mid gx = xg \text{ all } x \in G\},$$

and so we obtain from (3.1) an isomorphism $G/Z(G) \to \operatorname{Inn}(G)$. In fact, $\operatorname{Inn}(G)$ is a normal subgroup of $\operatorname{Aut}(G)$: for $g \in G$ and $\alpha \in \operatorname{Aut}(G)$,

$$(\alpha \circ i_g \circ \alpha^{-1})(x) = \alpha(g \cdot \alpha^{-1}(x) \cdot g^{-1}) = \alpha(g) \cdot x \cdot \alpha(g)^{-1},$$

and so $\alpha i_g \alpha^{-1} = i_{\alpha(g)}$.

A group G is said to be *complete* if the map $g \mapsto i_g : G \to \operatorname{Aut}(G)$ is an isomorphism. Note that this equivalent to the condition:

(a) the centre $Z(G)$ of G is trivial, and
(b) every automorphism of G is inner.

Example 3.9. (a) For $n \neq 2, 6$, S_n is complete. The group S_2 is commutative, hence $Z(S_2) \neq 1$, and for S_6, $\operatorname{Aut}(S_6)/\operatorname{Inn}(S_6) \approx C_2$. See Rotman 7.4, 7.8.

(b) Let[9] $G = \mathbb{F}_p^n$. The automorphisms of G as an abelian group are just the automorphisms of G as a vector space over $\mathbb{F}_p$; thus $\operatorname{Aut}(G) = \operatorname{GL}_n(\mathbb{F}_p)$. Because G is commutative, all automorphisms of G are outer (apart from the identity automorphism).

(c) As a particular case of (b), we see that

$$\operatorname{Aut}(C_2 \times C_2) = \operatorname{GL}_2(\mathbb{F}_2) \approx S_3.$$

Hence the nonisomorphic groups $C_2 \times C_2$ and S_3 have isomorphic automorphism groups.

(d) Let G be a cyclic group of order n, say $G = <g_0>$. An automorphism α of G must send g_0 to another generator of G. But g_0^m has order $\frac{n}{\gcd(m,n)}$, and so the generators of G are the elements g_0^m with $\gcd(m,n) = 1$. Thus $\alpha(g_0) = g_0^m$ for some m relatively prime to n, and in fact the map $\alpha \mapsto m$ defines an isomorphism

$$\operatorname{Aut}(C_n) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

where

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\text{units in the ring } \mathbb{Z}/n\mathbb{Z}\} = \{m + n\mathbb{Z} \mid \gcd(m,n) = 1\}.$$

This isomorphism is independent of the choice of a generator g_0 for G; in fact, if $\alpha(g_0) = g_0^m$, then for any other element $g = g_0^i$ of G,

$$\alpha(g) = \alpha(g_0^i) = \alpha(g_0)^i = g_0^{mi} = (g_0^i)^m = g^m.$$

(e) Since the centre of the quaternion group Q is $<a^2>$, we have that

$$\operatorname{Inn}(Q) = Q/ <a^2> \approx C_2 \times C_2.$$

In fact, $\operatorname{Aut}(Q) \approx S_4$. See Exercises.

(f) If G is a simple nonabelian group, then $\operatorname{Aut}(G)$ is complete. See Rotman 7.9.

[9] We use the standard (Bourbaki) notations: $\mathbb{N} = \{0, 1, 2, \ldots\}$, $\mathbb{Z}$ = ring of integers, $\mathbb{R}$ = field of real numbers, $\mathbb{C}$ = field of complex numbers, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ = field of p-elements, p prime.

Remark 3.10. It will be useful to have a description of $(\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Aut}(C_n)$. If $n = p_1^{r_1}\cdots p_s^{r_s}$ is the factorization of n into powers of distinct primes, then the Chinese Remainder Theorem (Dummit p268, Math 593(?)) gives us an isomorphism

$$\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}/p_1^{r_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_s^{r_s}\mathbb{Z},\quad m \mod n \mapsto (m \mod p_1^{r_1},\ldots,m \mod p_s^{r_s}),$$

which induces an isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \approx (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times\times\cdots\times(\mathbb{Z}/p_s^{r_s}\mathbb{Z})^\times.$$

Hence we need only consider the case $n = p^r$, p prime.

Suppose first that p is odd. The set $\{0,1,\ldots,p^r-1\}$ is a complete set of representatives for $\mathbb{Z}/p^r\mathbb{Z}$, and $\frac{1}{p}$ of these elements is divisible by p. Hence $(\mathbb{Z}/p^r\mathbb{Z})^\times$ has order $p^r - \frac{p^r}{p} = p^{r-1}(p-1)$. Because $p-1$ and p^r are relatively prime, we know from Math 593 that $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is isomorphic to the product of a group A of order $p-1$ and a group B of order p^{r-1}. The map

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times,$$

induces an isomorphism $A \to \mathbb{F}_p^\times$, and $\mathbb{F}_p^\times$, being a finite subgroup of the multiplicative group of a field, is cyclic (see the second part of the course). Thus $(\mathbb{Z}/p^r\mathbb{Z})^\times \supset A = <\zeta>$ for some element ζ of order $p-1$. Using the binomial theorem, one finds that $1+p$ has order p^{r-1} in $(\mathbb{Z}/p^r\mathbb{Z})^\times$, and therefore generates B. Thus $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic, with generator $\zeta(1+p)$, and every element can be written uniquely in the form

$$\zeta^i(1+p)^j,\quad 0\le i<p-1,\quad 0\le j<p^{r-1}.$$

On the other hand,

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar1,\bar3,\bar5,\bar7\} = <\bar3,\bar5> \approx C_2\times C_2$$

is not cyclic. The situation can be summarized by:

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \approx \begin{cases} C_{(p-1)p^{r-1}} & p \text{ odd},\\ C_2 & p^r = 2^2\\ C_2\times\ C_{2^{r-2}} & p=2, r>2.\end{cases}$$

See Dummit p308 for more details.

Definition 3.11. A subgroup H of a group G is called a *characteristic subgroup* if $\alpha(H) = H$ for all automorphisms α of G.

As for normal subgroups, it suffices to check that $\alpha(H)\subset H$ for all $\alpha\in\mathrm{Aut}(G)$.

Contrast: a subgroup H of G is normal if it is stable under all inner automorphisms of G; it is characteristic if it stable under all automorphisms.

Remark 3.12. (a) Consider groups $G \rhd H$. An inner automorphism restricts to an automorphism of H, which may be an outer automorphism of H. Thus a normal subgroup of H need not be a normal subgroup of G. However, a characteristic subgroup of H will be a normal subgroup of G. Also a characteristic subgroup of a characteristic subgroup is a characteristic subgroup.

(b) The centre $Z(G)$ of G is a characteristic subgroup, because

$$zg = gz \text{ all } g\in G \implies \alpha(z)\alpha(g) = \alpha(g)\alpha(z) \text{ all } g\in G,$$

and as g runs over G, $\alpha(g)$ also runs over G. In general, expect subgroups with a general group-theoretic definition to be characteristic.

(c) If H is the only subgroup of G of order m, then it must be characteristic, because $\alpha(H)$ is again a subgroup of G of order m.

(d) Every subgroup of an abelian group is normal, but such a subgroup need not be characteristic. For example, a subspace of dimension 1 in $G = \mathbb{F}_p^2$ will not be stable under $\mathrm{GL}_2(\mathbb{F}_p)$ and hence is not a characteristic subgroup.

3.4. Semidirect products. Let N be a normal subgroup of G. Each element g of G defines an automorphism of N, $n \mapsto gng^{-1}$, and so we have a homomorphism

$$\theta : G \to \mathrm{Aut}(N).$$

If there exists a subgroup Q of G such that the map $G \to G/N$ maps Q isomorphically onto G/N, then I claim that we can reconstruct G from the triple $(N, Q, \theta|Q)$. Indeed, for any $g \in G$, there exist unique elements $n \in N$, $q \in Q$, such that $g = nq$ (q is the element of Q representing g in G/N, and $n = gq^{-1}$), and so we have a one-to-one correspondence (of sets)

$$G \overset{1-1}{\leftrightarrow} N \times H.$$

If $g = nq$ and $g' = n'q'$, then

$$gg' = nqn'q' = n(qn'q^{-1})qq' = n \cdot \theta(q)(n') \cdot qq'.$$

Definition 3.13. A group G is said to be a *semidirect product* of the subgroups N and Q, written $N \rtimes Q$, if N is normal and $G \to G/N$ induces an isomorphism $Q \xrightarrow{\approx} G/N$. Equivalent condition: N and Q are subgroups of G such that

$$\text{(i) } N \lhd G;\ \text{(ii) } NQ = G;\ \text{(iii) } N \cap Q = \{1\}.$$

Note that Q need *not* be a normal subgroup of G.

Example 3.14. (a) In D_n, let $C_n = <\sigma>$ and $C_2 = <\tau>$; then

$$D_n = <\sigma> \rtimes <\tau> = C_n \rtimes C_2.$$

(b) The alternating subgroup A_n is a normal subgroup of S_n (because it has index 2), and $Q = \{(12)\} \xrightarrow{\approx} S_n/A_n$. Therefore $S_n = A_n \rtimes C_2$.

(c) The quaternion group is not a semidirect product. (See the exercises.)

(d) A cyclic group of order p^2, p prime, is not a semidirect product.

We have seen that, from a semidirect product $G = N \rtimes Q$, we obtain a triple

$$(N, Q, \theta : Q \to \mathrm{Aut}(N)).$$

We now prove that all triples (N, Q, θ) consisting of two groups N and Q and a homomorphism $\theta : Q \to \mathrm{Aut}(N)$ arise from semidirect products. As a set, let $G = N \times Q$, and define

$$(n, q)(n', q') = (n \cdot \theta(q)(n'), qq').$$

Proposition 3.15. *The above composition law makes G into a group, in fact, the semidirect product of N and Q.*

Proof. Write ${}^{q}n$ for $\theta(q)(n)$. First note that

$$((n,q),(n',q'))(n'',q'') = (n \cdot {}^{q}n' \cdot {}^{qq'}n'', qq'q'') = (n,q)((n',q')(n'',q''))$$

and so the product is associative. Clearly

$$(1,1)(n,q) = (n,q) = (n,q)(1,1)$$

and so $(1,1)$ is an identity element. Next

$$(n,q)({}^{q^{-1}}n, q^{-1}) = (1,1) = ({}^{q^{-1}}n, q^{-1})(n,q),$$

and so $({}^{q^{-1}}n, q^{-1})$ is an inverse for (n,q). Thus G is a group, and it easy to check that it satisfies the conditions (i,ii,iii) of (3.13). □

Write $G = N \rtimes_{\theta} Q$ for the above group.

Example 3.16. (a) Let θ be the (unique) nontrivial homomorphism $C_4 \to C_2 = \mathrm{Aut}(C_3)$, namely, that which sends a generator of C_4 to the map $x \mapsto x^2$. Then $G =_{df} C_3 \rtimes_{\theta} C_4$ is a noncommutative group of order 12, not isomorphic to A_4. If we denote the generators of C_3 and C_4 by a and b, then a and b generate G, and have the defining relations

$$a^3 = 1, \quad b^4 = 1, \quad bab^{-1} = a^2.$$

(b) Let N and Q be any two groups, and let θ be the trivial homomorphism $Q \to N$, i.e., $\theta(q) = 1$ for all $q \in Q$. Then

$$N \rtimes_{\theta} Q = N \times Q \qquad \text{(direct product)}.$$

(c) Both S_3 and C_6 are semidirect products of C_3 by C_2—they correspond to the two homomorphisms $C_2 \to C_2 = \mathrm{Aut}(C_3)$.

(d) Let $N =<a, b>$ be the product of two cyclic groups of order p with generators $a = \binom{1}{0}$ and $b = \binom{0}{1}$, and let Q be cyclic of order p with generator c. Define

$$\theta : Q \to \mathrm{Aut}\, N, \qquad c^i \mapsto \begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix}.$$

The group $G =_{df} N \rtimes_{\theta} Q$ is a group of order p^3, with generators a, b, c and defining relations

$$a^p = b^p = c^p = 1, \quad ab = cac^{-1}, \quad [b,a] = 1 = [b,c].$$

Because $b \neq a$, the group is noncommutative. When p is odd, all elements except 1 have order p. When $p = 2$, $G = D_4$. Note that this shows that a group can have quite different representations as a semidirect product:

$$D_4 = C_4 \rtimes C_2 = (C_2 \times C_2) \rtimes C_2.$$

(e) Let $N =<a>$ be cyclic of order p^2, and let $Q =<b>$ be cyclic of order p, where p is an odd prime. Then $\mathrm{Aut}\, N \approx C_{p-1} \times C_p$, and the generator of C_p is α where $\alpha(a) = a^{1+p}$ (hence $\alpha^2(a) = a^{1+2p}, \ldots$). Define $Q \to \mathrm{Aut}\, N$ by $b \mapsto \alpha$. The group $G =_{df} N \rtimes_{\theta} Q$ has generators a, b and defining relations

$$a^{p^2} = 1, \quad b^p = 1, \quad bab^{-1} = a^{1+p}.$$

It is a nonabelian group of order p^3, and possesses an element of order p^2.

For any odd prime p, the groups constructed in (d) and (e) are the only nonabelian groups of order p^3. (See later.)

(f) Let α be an automorphism of a group N. We can realize N as a normal subgroup of a group G in such a way that α becomes an inner automorphism $\alpha = i_g|N$, $g \in G$, in the bigger group. To see this, let $\theta : C_\infty \to \mathrm{Aut}(N)$ be the homomorphism sending a generator a of C_∞ to $\alpha \in \mathrm{Aut}(N)$, and let $G = N \rtimes_\theta C_\infty$. Then the element $g = (1, a)$ of G has the property that $g(n,1)g^{-1} = (\alpha(n), 1)$ for all $n \in N$.

3.5. Extensions of groups.

A sequence of groups and homomorphisms

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1$$

is *exact* if ι is injective, π is surjective, and $\mathrm{Ker}(\pi) = \mathrm{Im}(\iota)$. Thus $\iota(N)$ is a normal subgroup of G (isomorphic by ι to N) and $G/\iota(N) \xrightarrow{\approx} Q$. We often identify N with the subgroup $\iota(N)$ of G and Q with the quotient G/N.

An exact sequence as above is also referred to as an *extension of Q by N*. An extension is *central* if $\iota(N) \subset Z(G)$. For example,

$$1 \to N \to N \rtimes_\theta Q \to Q \to 1$$

is an extension of N by Q, which is central if (and only if) θ is the trivial homomorphism.

Two extensions of Q by N are isomorphic if there is a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d, equal] & G \arrow[r] \arrow[d, "\approx"] & Q \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & N \arrow[r] & G' \arrow[r] & Q \arrow[r] & 1.
\end{tikzcd}$$

An extension

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1$$

is said to be *split* if it isomorphic to a semidirect product. Equivalent conditions:

(a) there exists a subgroup $Q' \subset G$ such that π induces an isomorphism $Q' \to Q$; or
(b) there exists a homomorphism $s : Q \to G$ such that $\pi \circ s = \mathrm{id}$.

As we have seen (3.14c,d), in general an extension will not split. We list two criteria for this to happen.

Proposition 3.17 (Schur-Zassenhaus lemma). *An extension of finite groups of relatively prime order is split.*

Proof. Rotman 7.24. □

Proposition 3.18. *Let N be a normal subgroup of a group G. If N is complete, then G is the direct product of N with the centralizer*

$$C_G(N) =_{df} \{g \in G \mid gn = ng \text{ all } n \in N\}$$

of N in G.

Proof. Let $Q = C_G(N)$. Observe first that, for any $g \in G$, $n \mapsto gng^{-1} : N \to N$ is an automorphism of N, and (because N is complete), it must be the inner automorphism defined by an element $\gamma = \gamma(g)$ of N; thus

$$gng^{-1} = \gamma n \gamma^{-1} \quad \text{all } n \in N.$$

This equation shows that $\gamma^{-1}g \in Q$, and hence $g = \gamma(\gamma^{-1}g) \in NQ$. Since g was arbitrary, we have shown that $G = NQ$. Next note that any element of $N \cap Q$ is in the centre of N, which (by the completeness assumption) is trivial; hence $N \cap Q = 1$. Finally, for any element $g = nq \in G$,

$$gQg^{-1} = n(qQq^{-1})n^{-1} = nQn^{-1} = Q$$

(recall that every element of N commutes with every element of Q). Therefore Q is normal in G, and we have proved that N and Q satisfy the conditions of Proposition 3.6 and so $N \times Q \xrightarrow{\approx} G$. □

An extension gives rise to a homomorphism $\theta' : G \to \mathrm{Aut}(N)$, namely, $\theta'(g)(n) = gng^{-1}$. Let $\tilde{q} \in G$ map to q in Q; then the image of $\theta'(\tilde{q})$ in $\mathrm{Aut}(N)/\mathrm{Inn}(N)$ depends on q; therefore we get a homomorphism $\theta : Q \to \mathrm{Out}(N) =_{df} \mathrm{Aut}(N)/\mathrm{Inn}(N)$. This map θ depends only on the isomorphism class of the extension, and we write $\mathrm{Ext}^1(G, N)_\theta$ for the set of isomorphism classes of extensions with a given θ. These sets have been extensively studied.

3.6. The Hölder program.

Recall that a group G is simple if it contains no normal subgroup except 1 and G. In other words, a group is simple if it can't be realized as an extension of smaller groups. Every finite group can be obtained by taking repeated extensions of simple groups. Thus the simple finite groups can be regarded as the basic building blocks for all finite groups.

The problem of classifying all simple groups falls into two parts:

A. Classify all finite simple groups;
B. Classify all extensions of finite groups.

Part A has been solved: there is a complete list of finite simple groups. They are the cyclic groups of prime order, the alternating groups A_n for $n \geq 5$ (see the next section), certain infinite families of matrix groups, and the 26 "sporadic groups". As an example of a matrix group, consider

$$\mathrm{SL}_n(\mathbb{F}_q) =_{df} \{m \times m \text{ matrices } A \text{ with entries in } \mathbb{F}_q \text{ such that } \det A = 1\}.$$

Here $q = p^n$, p prime, and $\mathbb{F}_q$ is "the" field with q elements (see the second part of the course). This group is not simple, because the scalar matrices $\begin{pmatrix} \zeta & 0 & \cdots & 0 \\ 0 & \zeta & & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & \zeta \end{pmatrix}$, $\zeta^m = 1$, are in the centre. But they are the only matrices in centre, and for q and m sufficiently large (e.g., $q > 3$ when $m = 2$), the groups

$$\mathrm{PSL}_m(\mathbb{F}_q) =_{df} \mathrm{SL}_n(\mathbb{F}_q)/\{\text{centre}\}$$

are simple.

There are many results on Part B, and at least one expert has told me he considers it solved, but I'm sceptical.

4. Groups Acting on Sets

4.1. General definitions and results.

Definition 4.1. Let X be a set and let G be a group. A *left action* of G on X is a mapping $(g,x) \mapsto gx : G \times X \to X$ such that

(a) $1x = x$, for all $x \in X$;
(b) $(g_1 g_2)x = g_1(g_2 x)$, all g_1, $g_2 \in G$, $x \in X$.

The axioms imply that, for each $g \in G$, left translation by g,

$$g_L : X \to X, \quad x \mapsto gx,$$

has $(g^{-1})_L$ as an inverse, and therefore g_L is a bijection, i.e., $g_L \in \mathrm{Sym}(X)$. Axiom (b) now says that

$$g \mapsto g_L : G \to \mathrm{Sym}(X)$$

is a homomorphism. Thus, from a left action of G on X, we obtain a homomorphism $G \to \mathrm{Sym}(G)$, and conversely, such a homomorphism defines an action of G on X.

Example 4.2. (a) The symmetric group S_n acts on $\{1, 2, ..., n\}$. Every subgroup H of S_n acts on $\{1, 2, \ldots, n\}$.

(b) Every subgroup H of a group G acts on G by left translation,

$$H \times G \to G, \quad (h, x) \mapsto hx.$$

(c) Let H be a subgroup of G. If C is a left coset of H in G, then so also is gC for any $g \in G$. In this way, we get an action of G on the set of left cosets:

$$G \times G/H \to G/H, \quad (g, C) \mapsto gC.$$

(e) Every group G acts on itself by conjugation:

$$G \times G \to G, \quad (g, x) \mapsto {}^g x =_{df} gxg^{-1}.$$

For any normal subgroup N, G acts on N and G/N by conjugation.

(f) For any group G, $\mathrm{Aut}(G)$ acts on G.

A *right action* $X \times G \to G$ is defined similarly. To turn a right action into a left action, set $g * x = xg^{-1}$. For example, there is a natural right action of G on the set of right cosets of a subgroup H in G, namely, $(C, g) \mapsto Cg$, which can be turned into a left action $(g, C) \mapsto Cg^{-1}$.

A *morphism* of G-sets (better *G-map*; *G-equivariant map*) is a map $\varphi : X \to Y$ such that

$$\varphi(gx) = g\varphi(x), \quad \text{all } g \in G, \quad x \in X.$$

An *isomorphism* of G-sets is a bijective G-map; its inverse is then also a G-map.

Orbits. Let G act on X. A subset $S \subset X$ is said to be *stable* under the action of G if

$$g \in G, \quad x \in S \implies gx \in S.$$

The action of G on X then induces an action of G on S.

Write $x \sim_G y$ if $y = gx$, some $g \in G$. This relation is reflexive because $x = 1x$, symmetric because

$$y = gx \implies x = g^{-1}y$$

(multiply by g^{-1} on the left and use the axioms), and transitive because

$$y = gx, \quad z = g'y \implies z = g'(gx) = (g'g)x.$$

It is therefore an equivalence relation. The equivalence classes are called G-*orbits.* Thus the G-orbits partition X. Write $G\backslash X$ for the set of orbits.

By definition, the G-orbit containing x_0 is

$$Gx_0 =_{df} \{gx_0 \mid g \in G\}.$$

It is the smallest G-stable subset of X containing x_0.

Example 4.3. (a) Suppose G acts on X, and let $\alpha \in G$ be an element of order n. Then the orbits of $H =_{df} <\alpha> \in S_n$ are the sets of the form

$$\{x_0, \alpha x_0, \dots, \alpha^{n-1}x_0\}.$$

(These elements need not be distinct, and so the set may contain fewer than n elements.)

(b) The orbits for a subgroup H of G acting on G by left multiplication are the right cosets of H in G. We write $H\backslash G$ for the set of right cosets. Similarly, the orbits for H acting by right multiplication are the left cosets, and we write G/H for the set of left cosets. Note that the group law on G will *not* induce a group law on G/H unless H is normal.

(c) For a group G acting on itself by conjugation, the orbits are called *conjugacy classes:* for $x \in G$, the conjugacy class of x is the set $\{gxg^{-1} \mid g \in G\}$ of conjugates of x. The conjugacy class of x_0 consists only of x_0 if and only if x_0 is in the centre of G. In linear algebra the conjugacy classes in $G = \mathrm{GL}_n(k)$ are called similarity classes, and the theory of (rational) Jordan canonical forms provides a set of representatives for the conjugacy classes: two matrices are similar (conjugate) if and only if they have essentially the same Jordan canonical form. (See Math 593.)

Note that the stable subsets of X are precisely the sets that can be written as a union of orbits. For example, a subgroup H of G is normal if and only if it is a union of conjugacy classes.

The group G is said to act *transitively* on X if there is only one orbit, i.e., for any two elements x and y of X, there exists a $g \in G$ such that $gx = y$.

For example, S_n acts transitively on $\{1, 2, ...n\}$. For any subgroup H of a group G, G acts transitively on G/H. But G (almost) never acts transitively on G (or G/N or N) by conjugation.

The group G acts *doubly transitive* on X if for any two pairs (x, x'), (y, y') of elements of X, there exists a $g \in G$ such that $gx = y$, $gx' = y'$. Similarly define *k-fold transitivity,* $k \geq 3$.

Stabilizers. The *stabilizer* (or *isotropy group*) of an element $x \in X$ is

$$\mathrm{Stab}(x) = \{g \in G | gx = x\}.$$

It is a subgroup, but it need not be a normal subgroup. In fact:

Lemma 4.4. *If $y = gx$, then* $\mathrm{Stab}(y) = g \cdot \mathrm{Stab}(x) \cdot g^{-1}$.

Proof. Certainly, if $g'x = x$, then

$$(gg'g^{-1})y = gg'x = gx = y.$$

Hence $\mathrm{Stab}(y) \supset g \cdot \mathrm{Stab}(x) \cdot g^{-1}$. Conversely, if $g'y = y$, then

$$(g^{-1}g'g)x = g^{-1}g'(y) = g^{-1}y = x,$$

and so $g^{-1}g'g \in \mathrm{Stab}(x)$, i.e., $g' \in g \cdot \mathrm{Stab}(x) \cdot g^{-1}$. □

Clearly

$$\bigcap \mathrm{Stab}(x) = \mathrm{Ker}(G \to \mathrm{Sym}(X)),$$

which is a normal subgroup of G. If $\bigcap \mathrm{Stab}(x) = \{1\}$, i.e., $G \hookrightarrow \mathrm{Sym}(X)$, then G is said to act *effectively*. It acts *freely* if $\mathrm{Stab}(x) = 1$ for all $x \in X$, i.e., if $gx = x \implies g = 1$.

Example 4.5. (a) Let G act on G by conjugation. Then

$$\mathrm{Stab}(x) = \{g \in G \mid gx = xg\}.$$

This group is called the *centralizer* $C_G(x)$ of x in G. It consists of all elements of G that commute with, i.e., centralize, x. The intersection

$$\bigcap C_G(x) = \{g \in G \mid gx = xg \quad \forall x \in G\}$$

is a normal subgroup of G, called the *centre* of G. It consists of the elements of G that commute with every element of G.

(b) Let G act on G/H by left multiplication. Then $\mathrm{Stab}(H) = H$, and the stablizer of gH is gHg^{-1}.

Similarly, for a subset S of X, we define the *stabilizer* of S to be

$$\mathrm{Stab}(S) = \{g \in G \mid gS \subset S\}.$$

The same argument as before shows that

$$\mathrm{Stab}(gS) = g \cdot \mathrm{Stab}(S) \cdot g^{-1}.$$

Example 4.6. Let G act on G by conjugation, and let H be a subgroup of G. The stabilizer of H is called the *normalizer* $N_G(H)$ of H in G:

$$N_G(H) = \{g \in G \mid gHg^{-1} \subset H\}.$$

Clearly $N_G(H)$ is the largest subgroup of G containing H as a normal subgroup.

Transitive actions.

Proposition 4.7. *Suppose G acts transitively on X, and let $x_0 \in X$; then*

$$gH \mapsto gx_0 : G/\operatorname{Stab}(x_0) \to X$$

is an isomorphism of G-sets.

Proof. It is well-defined because if $h, h' \in \operatorname{Stab}(x_0)$, then $ghx_0 = gx_0 = gh'x_0$ for any $g \in G$. It is injective because

$$gx_0 = g'x_0 \implies g^{-1}g'x_0 = x_0 \implies g, g' \text{ lie in the same left coset of } \operatorname{Stab}(x_0).$$

It is surjective because G acts transitively. Finally, it is obviously G-equivariant. □

The isomorphism is *not canonical*: it depends on the choice of $x_0 \in X$. Thus to give a transitive action of G on a set X is *not* the same as to give a subgroup of G.

Corollary 4.8. *Let G act on X, and let $O = Gx_0$ be the orbit containing x_0. Then the number of elements in O,*

$$\#O = (G : \operatorname{Stab}(x_0)).$$

Proof. The action of G on O is transitive, and so $g \mapsto gx_0$ defines a bijection $G/\operatorname{Stab}(x_0) \to Gx_0$. □

This equation is frequently useful for computing $\#O$.

Proposition 4.9. *If G acts transitively on X, then, for any $x_0 \in X$,*

$$\operatorname{Ker}(G \to \operatorname{Sym}(X))$$

is the largest normal subgroup contained in $\operatorname{Stab}(x_0)$.

Proof. For any $x_0 \in X$, we know that $\operatorname{Ker}(G \to \operatorname{Sym}(X))$ is

$$\bigcap_{x \in X} \operatorname{Stab}(x) = \bigcap_{g \in G} \operatorname{Stab}(gx_0) = \bigcap g \cdot \operatorname{Stab}(x_0) \cdot g^{-1}.$$

Hence this is a consequence of the following lemma. □

Lemma 4.10. *For any subgroup H of a group G, $\bigcap_{g \in G} gHg^{-1}$ is the largest normal subgroup contained in H.*

Proof. First note that $N_0 =_{df} \bigcap_{g \in G} gHg^{-1}$, being an intersection of subgroups, is itself a subgroup. It is normal because

$$g_1 N_0 g_1^{-1} = \bigcap_{g \in G} (g_1 g) N_0 (g_1 g)^{-1} = N_0$$

—for the second equality, we used that, as g runs over the elements of G, so also does $g_1 g$. Thus N_0 is a normal subgroup of G contained in $1H1^{-1} = H$. If N is a second such group, then

$$N = gNg^{-1} \subset gHg^{-1}$$

for all $g \in G$, and so

$$N \subset \bigcap gHg^{-1} = N_0.$$

□

The class equation. Suppose X is finite; then X is a disjoint union of a finite number of orbits:

$$X = \bigcup_{i=1}^{m} O_i \qquad \text{(disjoint union)}.$$

Hence:

Proposition 4.11. *The number of elements in X is*

$$\#X = \sum_{i=1}^{m} \#O_i = \sum_{i=1}^{m} (G : \mathrm{Stab}(x_i)), \quad x_i \text{ in } O_i.$$

In the case that G is acting on itself by conjugation, this formula reads:

Proposition 4.12 (Class equation).

$$(G : 1) = \sum (G : C_G(x))$$

(x runs over a set of representatives for the conjugacy classes), or

$$(G : 1) = (Z(G) : 1) + \sum (G : C_G(y))$$

(y runs over set of representatives for the conjugacy classes containing more than one element).

Theorem 4.13 (Cauchy). *If the prime p divides $(G : 1)$, then G contains an element of order p.*

Proof. We use induction on $(G : 1)$. If for some y not in the centre of G, p does not divide $(G : C_G(y))$, then $p|C_G(y)$ and we can apply induction to find an element of order p in $C_G(y)$. Thus we may suppose that p divides all of the terms $(G : C_G(y))$ in the class equation (second form), and so also divides $Z(G)$. But $Z(G)$ is commutative, and it follows from the structure theory of such groups (for example) that $Z(G)$ will contain an element of order p. □

p-groups.

Theorem 4.14. *A finite p-group $\neq 1$ has centre $\neq \{1\}$.*

Proof. By assumption, $(G : 1)$ is a power of p, and it follows that $(G : C_G(y))$ is power of p ($\neq p^0$) for all y in the above sum. Since every other term in the sum is divisible by p, so also is $(Z(G) : 1)$. □

Corollary 4.15. *A group of order p^m has normal subgroups of order p^n for all $n \leq m$.*

Proof. We use induction on m. The centre of G contains an element g of order p, and so $N = <g>$ is a normal subgroup of G of order p. Now the induction hypothesis allows us to assume the result for G/N, and the correspondence theorem (3.3) then gives it to us for G. □

Proposition 4.16. *A group of order p^2 is commutative, and hence is isomorphic to $C_p \times C_p$ or C_{p^2}.*

Proof. We know that the centre Z is nontrivial, and that G/Z therefore has order 1 or p. In either case it is cyclic, and the next result implies that G is commutative. □

Lemma 4.17. *Suppose G contains a subgroup H in its centre (hence H is normal) such that G/H is cyclic. Then G is commutative.*

Proof. Let $a \in G$ be such that aH generates G/H, so that $G/H = \{(aH)^i \mid i \in \mathbb{Z}\}$. Since $(aH)^i = a^iH$, we see that every element of G can be written $g = a^ih$ with $h \in H$, $i \in \mathbb{Z}$. Now

$$\begin{aligned} a^ih \cdot a^{i'}h' &= a^ia^{i'}hh' \qquad \text{because } H \subset Z(G) \\ &= a^{i'}a^ih'h \\ &= a^{i'}h' \cdot a^ih. \end{aligned}$$

□

Remark 4.18. The above proof shows that if $H \subset Z(G)$ and G contains a set of representatives for G/H whose elements commute, then G is commutative.

It is now not difficult to show that any noncommutative group of order p^3 is isomorphic to one of the groups constructed in (3.16d,e) (see exercises). Thus, up to isomorphism, there are exactly two noncommutative groups of order p^3.

Action on the left cosets. The action of G on the set of left cosets G/H of H in G is a very useful tool in the study of groups. We illustrate this with some examples.

Let $X = G/H$. Recall that, for any $g \in G$,

$$\mathrm{Stab}(gH) = g\,\mathrm{Stab}(H)g^{-1} = gHg^{-1}$$

and the kernel of

$$G \to \mathrm{Sym}(X)$$

is the largest normal subgroup $\bigcap_{g\in G} gHg^{-1}$ of G contained in H.

Remark 4.19. (a) Let H be a subgroup of G not containing a normal subgroup of G other than 1. Then $G \to \mathrm{Sym}(G/H)$ will be injective, and we will have realized G as a subgroup of a symmetric group of order much smaller than $(G:1)!$. For example, if G is simple, then the Sylow theorems imply that G has many proper subgroups $H \neq 1$ (unless G is cyclic), but (by definition) it has no such normal subgroup.

(b) If $(G:1)$ does not divide $(G:H)!$, then

$$G \to \mathrm{Sym}(G/H)$$

can't be injective (Lagrange's theorem), and we can conclude that H contains a normal subgroup $\neq 1$ of G. For example, if G has order 99, then it will have a subgroup of order 11 (Cauchy's theorem), and the subgroup must be normal. In fact, $G = N \times Q$.

Example 4.20. Let G be a group of order 6. According to Cauchy's theorem, G must contain an element σ of order 3 and an element τ of order 2. Moreover $N =_{df} <\sigma>$ must be normal because $6 \not| 2!$ (or simply because it has index 2). Let $H = <\tau>$.

Either (a) H is normal in G, or (b) H is not normal in G. In the first case, $\sigma\tau\sigma^{-1} = \tau$, i.e., $\sigma\tau = \tau\sigma$, and so (4.17) shows that G is commutative, $G \approx C_2 \times C_3$. In the second case, $G \to \mathrm{Sym}(G/H)$ is injective, hence surjective, and so $G \approx S_3$. We have succeeded in classifying the groups of order 6.

4.2. Permutation groups.

Consider $\mathrm{Sym}(X)$ where X has n elements. Since (up to isomorphism) a symmetry group $\mathrm{Sym}(X)$ depends only on the number of elements in X, we may take $X = \{1, 2, \ldots, n\}$, and so work with[10] S_n. Consider a permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \ldots & \alpha(n) \end{pmatrix}.$$

Then α is said to be *even* or *odd* according as the number of pairs (i, j) with $i < j$ and $\alpha(i) > \alpha(j)$ is even or odd. The *signature*, $\mathrm{sign}(\alpha)$, of α is $+1$ or -1 according as α is even or odd. [Picture.]

For any polynomial $F(X_1, ..., X_n)$ and permutation α of $\{1, \ldots, n\}$, define

$$(\alpha F)(X_1, ..., X_n) = F(X_{\alpha(1)}, ..., X_{\alpha(n)}),$$

i.e., αF is obtained from F by replacing each X_i with $X_{\alpha(i)}$. Note that

$$(\alpha\beta F)(X_1, ..., X_n) = F(X_{\alpha\beta(1)}, \ldots) = F(X_{\alpha(\beta(1))}, \ldots) = (\alpha(\beta F))(X_1, ..., X_n).$$

Let $G(X_1, ..., X_n) = \prod_{i<j}(X_j - X_i)$. Then

$$(\alpha G)(X_1, ..., X_n) = \prod_{i<j}(X_{\alpha(j)} - X_{\alpha(i)}).$$

Hence $\alpha G = \mathrm{sign}(\alpha) \cdot G$. By definition $\alpha\beta G = \mathrm{sign}(\alpha\beta)G$, and

$$\alpha\beta G = \alpha(\beta G) = \alpha(\mathrm{sign}(\beta)G) = \mathrm{sign}\,\beta(\alpha G) = \mathrm{sign}(\alpha)\,\mathrm{sign}(\beta)G.$$

Hence $\mathrm{sign}(\alpha\beta) = \mathrm{sign}\,\alpha\,\mathrm{sign}\,\beta$, and we have shown that "sign" is a homomorphism $S_n \to \{\pm 1\}$. Its kernel is a normal subgroup of S_n of order $\frac{n!}{2}$, called the *alternating group* A_n.

A *cycle* is a permutation of the following form

$$i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_r \mapsto i_1, \quad \text{remaining } i\text{'s fixed.}$$

We denote it by $(i_1 i_2 ... i_r)$, and call r its *length*—note that r is also its order. A cycle of length 2 is called a *transposition.* A cycle (i) of length 1 is the identity map. The *support* of the cycle $(i_1 \ldots i_r)$ is the set $\{i_1, \ldots, i_r\}$, and cycles are said to be *disjoint* if their supports are disjoint. Note that disjoint cycles commute. If

$$\alpha = (i_1 ... i_r)(j_1 ... j_s) \cdots (l_1 ... l_u) \qquad \text{(disjoint cycles)},$$

then

$$\alpha^m = (i_1 ... i_r)^m (j_1 ... j_s)^m \cdots (l_1 ... l_u)^m \qquad \text{(disjoint cycles)},$$

and it follows that α has order $\mathrm{lcm}(r, s, ..., u)$.

Proposition 4.21. *Every permutation can be written (essentially uniquely) as a product of disjoint cycles.*

[10] We of course, define multiplication in S_n to be composition; other authors (e.g., M. Artin) unaccountably write things backwards.

Proof. Let $\alpha \in S_n$, and let $O \subset \{1, 2, \ldots, n\}$ be an orbit for $<\alpha>$. For any $i \in O$, $O = \{i, \alpha(i), \ldots, \alpha^{r-1}(i)\}$. Therefore α and the cycle $(i\,\alpha(i)\ \ldots\ \alpha^{r-1}(i))$ have the same action on any element of O. Let

$$\{1, 2, \ldots, n\} = \bigcup_{j=1}^{m} O_j$$

be a the decomposition of $\{1, \ldots, n\}$ into a disjoint union of orbits for $<\alpha>$, and let γ_j be the cycle associated with O_j. Then

$$\alpha = \gamma_1 \cdots \gamma_m$$

is a decomposition of α into a product of disjoint cycles. For the uniqueness, note that a decomposition $\alpha = \gamma_1 \cdots \gamma_m$ into a product of disjoint cycles must correspond to a decomposition of $\{1, ..., n\}$ into orbits (ignoring cycles of length 1 and orbits with only one element). We can drop cycles of length one, change the order of the cycles, and change how we write each cycle, but that's all because the orbits are intrinsically attached to α. □

For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 4 & 9 & 1 & 3 & 6 & 8 & 2 \end{pmatrix} = (15)(276349)(8)$$

It has order $\mathrm{lcm}(2, 5) = 10$.

Corollary 4.22. *A permutation can be written as a product of transpositions; the number of transpositions is even or odd according as α is even or odd.*

Proof. The cycle

$$(i_1 i_2 ... i_r) = (i_1 i_2) \cdots (i_{r-2} i_{r-1})(i_{r-1} i_r),$$

and so the first statement follows from the proposition. Because sign is a homomorphism, and the signature of a transposition is -1, $\mathrm{sign}(\alpha) = (-1)^{\#\mathrm{transpositions}}$. □

Note that the formula in the proof shows that the signature of a cycle of length r is $(-1)^{r-1}$, i.e., an r-cycle is even or odd according as r is odd or even.

It is possible to define a permutation to be even or odd according as it is a product of an even or odd number of transpositions, but then one has to go through an argument as above to show that this is a well-defined notion.

The corollary says that S_n is generated by transpositions. For A_n there is the following result.

Corollary 4.23. *The alternating group A_n is generated by cycles of length three.*

Proof. Any $\alpha \in A_n$ is the product of an even number of transpositions, $\alpha = t_1 t_1' \cdots t_m t_m'$, but the product of two transpositions can always be written as a product of 3-cycles:

$$(ij)(kl) = \begin{cases} (ij)(jl) = (ijl) & \text{case } j = k, \\ (ij)(jk)(jk)(kl) = (ijk)(jkl) & \text{case } i, j, k, l \text{ distinct}, \\ 1 & \text{case } (ij) = (kl). \end{cases}$$

□

Recall that two elements a and b of a group G are said to be conjugate $a \sim b$ if there exists an element $g \in G$ such that $b = gag^{-1}$, and that conjugacy is an equivalence relation. For any group G, it is useful to determine the conjugacy classes in G.

Example 4.24. In S_n, the conjugate of a cycle is given by:

$$g(i_1 \dots i_k)g^{-1} = (g(i_1) \dots g(i_k)).$$

Hence $g(i_1 \dots i_r)(j_1 \dots j_s) \dots (l_1 \dots l_u)g^{-1} = (g(i_1) \dots g(i_r))(g(j_1) \dots g(j_s)) \dots (g(l_1)...g(l_u))$ (even if the cycles are not disjoint). In other words, to obtain $g\alpha g^{-1}$, replace each element in a cycle of α be its image under g.

We shall now determine the conjugacy classes in S_n. By a *partition* of n, we mean a sequence of integers $n_1, \dots, n_k$ such that $1 \leq n_i \leq n_{i+1} \leq n$ (all i) and

$$n_1 + n_2 + \cdots + n_k = n.$$

Thus there are 1, 2, 3, 5, 7, 11, ... partitions of 1, 2, 3, 4, 5, 6, ... respectively (and 1, 121, 505 partitions of 61). Note that a partition

$$\{1, 2, ..., n\} = O_1 \cup ... \cup O_k \qquad \text{(disjoint union)}$$

of $\{1, 2, \dots, n\}$ determines a partition of n,

$$n = n_1 + n_2 + ... + n_k, \quad n_i = \#(O_i).$$

Since the orbits of an element α of S_n form a partition of $\{1, \dots, n\}$, we can attach to each such α a partition of n. For example, if

$$\alpha = (i_1 \dots i_{n_1}) \cdots (l_1 \dots l_{n_k}), \quad \text{(disjoint cycles)} \quad 1 < n_i \leq n_{i+1},$$

then the partition of n attached to α is

$$1, 1, \dots, 1, n_1, \dots, n_k \qquad (n - \sum n_i \text{ ones}).$$

Proposition 4.25. *Two elements α and β of S_n are conjugate if and only if they define the same partitions of n.*

Proof. $\Longleftarrow$: Since α and β define the same partitions of n, their decompositions into products of disjoint cycles have the same type:

$$\alpha = (i_1 \dots i_r)(j_1 \dots j_s) \dots (l_1 \dots l_u),$$

$$\beta = (i'_1 \dots i'_r)(j'_1 \dots j'_s) \dots (l'_1 \dots l'_u).$$

If we define g to be

$$\begin{pmatrix} i_1 & \cdots & i_r & j_1 & \cdots & j_s & \cdots & l_1 & \cdots & l_u \\ i'_1 & \cdots & i'_r & j'_1 & \cdots & j'_s & \cdots & l'_1 & \cdots & l'_u \end{pmatrix}$$

then

$$g\alpha g^{-1} = \beta.$$

$\Longrightarrow$: It follows from the calculation in (4.24) that conjugating an element preserves the type of its disjoint cycle decomposition. □

Example 4.26. $(ijk) = \binom{1234...}{ijk4...}(123)\binom{1234...}{ijk4...}^{-1}$.

Remark 4.27. For $1 < k \leq n$, there are $\frac{n(n-1)\cdots(n-k+1)}{k}$ distinct k-cycles in S_n. The $\frac{1}{k}$ is needed so that we don't count

$$(i_1 i_2 \ldots i_k) = (i_k i_1 \ldots i_{k-1}) = \ldots$$

k times. Similarly, it is possible to compute the number of elements in any conjugacy class in S_n, but a little care is needed when the partition of n has several terms equal. For example, the number of permutations in S_4 of type $(ab)(cd)$ is

$$\frac{1}{2}\left(\frac{4\times 3}{2}\times\frac{2\times 1}{2}\right) = 3.$$

The $\frac{1}{2}$ is needed so that we don't count $(ab)(cd) = (cd)(ab)$ twice. For S_4 we have the following table:

Partition	Element	No. in Conj. Class	Parity
$1+1+1+1$	1	1	even
$1+1+2$	(ab)	6	odd
$1+3$	(abc)	8	even
$2+2$	$(ab)(cd)$	3	even
4	$(abcd)$	6	odd

Note that A_4 contains exactly 3 elements of order 2, namely those of type $2+2$, and that together with 1 they form a subgroup V. This group is a union of conjugacy classes, and is therefore a normal subgroup of S_4.

Theorem 4.28 (Galois). *The group A_n is simple if $n \geq 5$*

Remark 4.29. For $n = 2$, A_n is trivial, and for $n = 3$, A_n is cyclic of order 3, and hence simple; for $n = 4$ it is nonabelian and nonsimple (it contains the normal (even characteristic) subgroup V—see above).

Lemma 4.30. *Let N be a normal subgroup of A_n ($n \geq 5$); if N contains a cycle of length three, then it contains all cycles of length three, and so equals A_n.*

Proof. Let γ be the cycle of length three in N, and let α be a second cycle of length three in A_n. We know that $\alpha = g\gamma g^{-1}$ for some $g \in S_n$. If $g \in A_n$, then this shows that α is also in N. If not, because $n \geq 5$, there exists a transposition $t \in S_n$ disjoint from α, and then

$$\alpha = t\alpha t^{-1} = tg\gamma g^{-1}t^{-1}, \qquad tg \in A_n,$$

and so again $\alpha \in N$. □

The next lemma completes the proof of the Theorem.

Lemma 4.31. *Every normal subgroup N of A_n, $n \geq 5$, $N \neq 1$, contains a cycle of length* 3.

Proof. Let $\alpha \in N$, $\alpha \neq 1$. If α is not a 3-cycle, we shall construct another element $\alpha' \in N$, $\alpha' \neq 1$, which fixes more elements of $\{1, 2, \ldots, n\}$ than does α. If α' is not a 3-cycle, then we can apply the same construction. After a finite number of steps, we arrive at a 3-cycle.

Suppose α is not a 3-cycle. When we express it as a product of disjoint cycles, either it contains a cycle of length ≥ 3 or else it is a product of transpositions, say

(i) $\alpha = (i_1 i_2 i_3 ...)\cdots$ or
(ii) $\alpha = (i_1 i_2)(i_3 i_4)\cdots$.

In the first case, α moves two numbers, say i_4, i_5, other than i_1, i_2, i_3, because $\alpha \neq (i_1 \dots i_4)$. Let $\gamma = (i_3 i_4 i_5)$. Then $\alpha_1 =_{df} \gamma\alpha\gamma^{-1} = (i_1 i_2 i_4 \dots)\cdots \in N$, and is distinct from α (because it acts differently on i_2). Thus $\alpha' =_{df} \alpha_1\alpha^{-1} \neq 1$, but $\alpha' = \gamma\alpha\gamma^{-1}\alpha^{-1}$ fixes i_2 and all elements other than $i_1, \dots, i_5$ fixed by α—it therefore fixes more elements than α.

In the second case, form γ, α_1, α_2 as before with i_4 as in (ii) and i_5 any element distinct from i_1, i_2, i_3, i_4. Then $\alpha_1 = (i_1 i_2)(i_4 i_5)\cdots$ is distinct from α because it acts differently on i_4. Thus $\alpha' = \alpha_1\alpha^{-1} \neq 1$, but α' fixes i_1 and i_2, and all elements $\neq i_1, \dots, i_5$ not fixed by α—it therefore fixes at least one more element than α. □

Corollary 4.32. *For $n \geq 5$, the only normal subgroups of S_n are 1, A_n, and S_n.*

Proof. If N is normal in S_n, then $N \cap A_n$ is normal in A_n. Therefore either $N \cap A_n = A_n$ or $N \cap A_n = \{1\}$. In the first case, $N \supset A_n$, which has index 2 in S_n, and so $N = A_n$ or S_n. In the second case, the map $x \mapsto xA_n : N \to S_n/A_n$ is injective, and so N has order 1 or 2, but it can't have order 2 because no conjugacy class in S_n (other than $\{1\}$) consists of a single element. □

Remark 4.33. A group G is said to be *solvable* if there exist subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset G_3 \supset \cdots \supset G_r = \{1\}$$

such that each G_i is normal in G_{i-1} and the quotient G_{i-1}/G_i is abelian. Thus A_n (also S_n) is not solvable if $n \geq 5$.

Let $f(X) \in \mathbb{Q}[X]$ be of degree n. In the second part of the course, we shall attach to f a subgroup of the group of permutations of the roots of f, $G_f \subset S_n$, and we shall show that the roots of f can be obtained from the coefficients of f by extracting radicals if and only if G_f is solvable. We shall see, that there exist (lots of) polynomials of all degrees with $G_f = S_n$.

4.3. The Todd-Coxeter algorithm.

Let G be a group described by a finite presentation, and let H be a subgroup described by a generating set. Then the Todd-Coxeter algorithm [11] is a strategy for writing down the set of left cosets of H in G together with the action of G on the set. I illustrate it with an example (see M. Artin, *Algebra,* 6.9 for more details, but note that he composes permutations backwards).

Let $G = <a, b, c | a^3, b^2, c^2, cba>$ and let H be the subgroup generated by c (strictly speaking, H is the subgroup generated by the element of G represented by the reduced word c). The operation of G on the set of cosets is described by the action of the generators, which must satisfy the following rules:

(i) Each generator (a, b, c in our example) acts as a permutation.
(ii) The relations (a^3, b^2, c^2, cba in our example) act trivially.
(iii) The generators of H (c in our example) fix the coset $1H$.
(iv) The operation on the cosets is transitive.

[11] To solve a problem, an algorithm must always terminate in a finite time with the correct answer to the problem. The Todd-Coxeter algorithm does not solve the problem of determining whether a finite presentation defines a finite group (in fact, there is no such algorithm). It does, however, solve the problem of determining the order of a finite group from a finite presentation of the group (use the algorithm with H the trivial subgroup 1.)

The strategy is to introduce cosets, denoted $1, 2, \ldots$ with $1 = 1H$, as necessary.

Rule (iii) tells us simply that $c1 = c$. We now apply the first two rules. Since we don't what $a1$ is, let's denote it 2: $a1 = 2$. Similarly, let $a2 = 3$. Now $a3 = a^3 1$, which according to (ii) must be 1. Thus, we have introduce three (potential) cosets 1,2,3, permuted by a as follows:

$$1 \xrightarrow{a} 2 \xrightarrow{a} 3 \xrightarrow{a} 1.$$

What is $b1$? We don't know, and so it is prudent to introduce another coset $4 = b1$. Now $b4 = 1$, and so we have

$$1 \xrightarrow{b} 4 \xrightarrow{b} 1.$$

We still have the relation cba. We know $a1 = 2$, but we don't know what $b2$ is, and so set $b2 = 5$. By (iii) $c1 = 1$, and by (ii) applied to cba we have $c5 = 1$. Therefore, according to (i) we must have $5 = 1$; we drop 5, and so now $b2 = 1$. Since $b4 = 1$ we must have $4 = 2$, and so we can drop 4 also. What we know can be summarized by the table:

	a	a	a	b	b	c	c	a	b	c
1	2	3	1	2	1	1	1	2	1	1
2	3	1	2	1	2		2	3		2
3	1	2	3		3		3	1	2	3

The bottom right corner, which is forced by (ii), tells us that $c2 = 3$. This then determines the rest of the table:

	a	a	a	b	b	c	c	a	b	c
1	2	3	1	2	1	1	1	2	1	1
2	3	1	2	1	2	3	2	3	3	2
3	1	2	3	3	3	2	3	1	2	3

We find that we have three cosets on which a, b, c act as

$$a = (123) \quad b = (12) \quad c = (23).$$

More precisely, we have written down a map $G \to S_3$ that is consistent with the above rules. A theorem (Artin, ibid.) now says that this does in fact describe the action of G on G/H. Since the three elements (123), (12), and (23) generate S_3, this shows that the action of G on G/H induces an isomorphism $G \to S_3$, and that H is a subgroup of order 2.

In (Artin, ibid.) it is explained how to make this procedure into an algorithm which, when it succeeds in producing a consistent table, will in fact produce the correct table.

This algorithm is implemented in Maple, except that it computes the action the *right* cosets. Here is a transcript: `>with(group); [loads the group theory package.]`

```
>G:=grelgroup({a,b,c},{[a,a,a],[b,b],[c,c],[a,b,c]}); [defines G to have
generators a,b,c and relations aaa, bb, cc, abc]

>H:=subgrel({x=[c]},G); [defines H to be the subgroup generated by c]

>permrep(H);

permgroup(3, a=[[1,2,3],b=[1,2],c=[2,3]])

[computes the action of G on the set of right cosets of H in G].
```

4.4. Primitive actions.

Let G be a group acting on a set X, and let π be a partition of X. We say that π is *stabilized* by G if

$$A \in \pi \implies gA \in \pi \text{ for each } A \in \pi.$$

Example 4.34. (a) The subgroup $G =< (1234) >$ of S_4 stabilizes the partition $\{\{1,3\},\{2,4\}\}$ of $\{1,2,3,4\}$.

(b) Let $X = \{1,2,3,4\}$ be identified with the set of vertices of the square on which D_4 acts in the usual way, namely, $\sigma = (1234)$, $\tau = (2,4)$. Then D_4 stabilizes the partition $\{\{1,3\},\{2,4\}\}$.

(c) Let X be the set of partitions of $\{1,2,3,4\}$ into two sets, each with two elements. Then S_4 acts on X, and $\text{Ker}(S_4 \to \text{Sym}(X)) = V$. See (4.27).

The group G always stabilizes the trivial partitions of X, namely, the set of all one-element subsets of X, and $\{X\}$. If it stabilizes only those partitions, we say that the action is *primitive.* A subgroup of $\text{Sym}(X)$ is said to be *primitive* if it acts primitively on X. For example, a subgroup of S_n is primitive if it acts primitively on $\{1,2,\ldots,n\}$. In particular, S_n is primitive, but D_4, regarded as a subgroup of S_4 in the obvious way, is not primitive.

Example 4.35. A doubly transitive action is primitive: if it stabilized $\{\{x,x',...\},\{y,...\}...\}$ then there would be no element sending (x,x') to (x,y).

Remark 4.36. The G-orbits form a partition of X that is stabilized by G. If the action is primitive, then the partition of orbits must be one of the trivial ones. Hence

$$\text{primitive} \implies \text{action transitive or trivial } (gx = x \text{ all } g, x).$$

For the remainder of this section, G is a finite group acting transitively on a set X with at least two elements.

Proposition 4.37. *The group G acts imprimitively if and only if there is an*

$$A \subset X, \quad A \neq X, \quad \#A \geq 2,$$

such that, for each $g \in G$, $gA = A$ or $gA \cap A = \emptyset$.

Proof. $\implies$: The partition π stablized by G contains such an A.

$\impliedby$: Suppose we have such an A. We can form a partition $\{A, g_1A, g_2A, ..., B\}$ where $B = X - \bigcup gA = \emptyset$ (because G acts transitively). It is stabilized by G. □

A subset A of X such that, for each $g \in G$, $gA = A$ or $gA \cap A = \emptyset$ is called *block.*

Proposition 4.38. *Let A be a block in X with $\#A \geq 2$, $A \neq X$. For any $x \in A$,*

$$\text{Stab}(x) \subsetneqq \text{Stab}(A) \subsetneqq G.$$

Proof. We have $\text{Stab}(A) \supset \text{Stab}(x)$ because

$$gx = x \implies gA \cap A \neq \emptyset \implies gA = A.$$

Let $y \in A$, $y \neq x$. Because G acts transitively on X, there is a $g \in G$ such that $gx = y$. Then $g \in \text{Stab}(A)$, but $g \notin \text{Stab}(x)$.

Let $y \notin A$. There is a $g \in G$ such that $gx = y$, and then $g \notin \text{Stab}(A)$. □

Theorem 4.39. *Under the above assumptions, G acts primitively on $X \iff \mathrm{Stab}(x)$ is a maximal subgroup of G for one (hence all) $x \in X$.*

Proof. If G does not act primitively on X, then (see 4.37) there is a block $A \subsetneqq X$ with at least two elements, and so (4.38) shows that $\mathrm{Stab}(x)$ will not be maximal for any $x \in A$.

Conversely, if there exists an x in X and a group H such that

$$\mathrm{Stab}(x) \subsetneqq H \subsetneqq G$$

then I claim that $A = Hx$ is a block $\neq X$ with at least two elements.

Because G acts transitively on X, $G/\mathrm{Stab}(x) \xrightarrow{\approx} X$, and so $H \neq \mathrm{Stab}(x) \implies Hx \neq \{x\}$. Hence the condition on H implies $\{x\} \subsetneqq A \subsetneqq X$.

If $g \in H$, then $gA = A$. If $g \notin H$, then gA is disjoint from A: for suppose $ghx = h'x$; then $h'^{-1}gh \in \mathrm{Stab}(x) \subset H$, say $h'^{-1}gh = h''$, and $g = h'h''h^{-1} \in H$. □

5. The Sylow Theorems; Applications

In this section, all groups are finite. If p^r is the highest power of the prime p dividing $(G:1)$, then a subgroup of G of order p^r is called a *Sylow p-subgroup of G*. The Sylow theorems state that there exist Sylow p-subgroups for all primes p dividing $(G:1)$, that all Sylow p-subgroups for a fixed p are conjugate, and that every p-subgroup of G is contained in such a subgroup; moreover, the theorems restrict the possible number of Sylow p-subgroups in G.

5.1. The Sylow theorems.

In the proofs, we frequently use that if O is an orbit for a group H acting on a set X, and $x_0 \in O$, then the map $H \to X$, $g \mapsto hx_0$ induces a bijection

$$H/\operatorname{Stab}(x_0) \to O;$$

see (4.7). Therefore

$$(H : \operatorname{Stab}(x_0)) = \#O.$$

In particular, if H is a p-group, then $\#O$ is a power of p: either O consists of a single element, or $\#O$ is divisible by p. Since X is a disjoint union of the orbits, we can conclude:

Lemma 5.1. *Let H be a p-group acting on a finite set X, and let X^H be the set of points fixed by H; then $\#X \equiv \#X^H$ (mod p).*

When the lemma is applied to a p-group H acting on itself by conjugation, we find that

$$(Z(H):1) \equiv (H:1) \mod p$$

because the orbits in this case are the conjugacy classes, and the conjugacy class of h consists only of h if and only if h is in the centre of H.

Theorem 5.2 (Sylow I). *Let G be a finite group, and let p be prime. If $p^r|(G:1)$, then G has a subgroup of order p^r.*

Proof. According to (4.15), it suffices to prove this with p^r the highest power of p dividing $(G:1)$, and so from now on we assume that $(G:1) = p^r m$ with m not divisible by p. Let

$$X = \{\text{sub}\textit{sets} \text{ of } G \text{ with } p^r \text{ elements}\},$$

with the action of G defined by

$$G \times X \to X, \quad (g, A) \mapsto gA =_{df} \{ga \mid a \in A\}.$$

Let $A \in X$, and let

$$H = \operatorname{Stab}(A) =_{df} \{g \in G \mid gA \subset A\}.$$

For any $a_0 \in A$, $h \mapsto ha_0 : H \to A$ is injective, and so $(H:1) \le \#A = p^r$. Consider

$$(G:H) = (G:H)(H:1).$$

We know $p^r|(G:H)$, $(H:1) \le p^r$, and $(G:H) = \#O$ where O is the orbit of A. If we can find an A such that p doesn't divide $\#O$, then we can conclude that (for such an A), $H = \operatorname{Stab} A$ has order p^r.

The number of elements in X is

$$\#X = \binom{p^r m}{p^r} = \frac{(p^r m)(p^r m-1)\cdots(p^r m-i)\cdots(p^r m-p^r+1)}{p^r(p^r-1)\cdots(p^r-i)\cdots(p^r-p^r+1)}.$$

Note that, because $i < p^r$, the power of p dividing $p^r m - i$ is the power of p dividing i. The same is true of $p^r - i$. Therefore the corresponding terms on top and bottom are divisible by the same powers of p, and so p does not divide $\#X$. Because the orbits form a partition of X,

$$\#X = \sum \#O_i, \quad O_i \text{ the distinct orbits,}$$

at least one of the $\#O_i$ is not divisible by p. □

Remark 5.3. The proof can be modified to show directly that for each power p^r of p dividing $(G:1)$, there is a subgroup H of G of order p^r. One again writes $(G:1) = p^r m$ and considers the set X of all subsets of order p^r. In this case, $\#X$ is divisible by the highest power p^{r_0} of p dividing m, but not by p^{r_0+1}, and it follows that there is an $A \in X$ the number of elements in whose orbit is not divisible by p^{r_0+1}. For such an A, the same counting argument shows that $\mathrm{Stab}(A)$ has p^r elements.

We obtain another proof of Cauchy's theorem.

Corollary 5.4 (Cauchy). *If a prime p divides $(G:1)$, then G has an element of order p.*

Proof. We have to show that a p-group $H \neq 1$ contains an element of order p. But any element $g \neq 1$ of such an H is of order p^m for some $m \geq 1$, and $g^{p^{m-1}}$ will have order p. □

Example 5.5. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field with p elements, and let $G = \mathrm{GL}_n(\mathbb{F}_p)$. Then the order of G is

$$(p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1}).$$

Therefore the power of p dividing $(G:1)$ is $p^{1+2+\cdots+(n-1)}$. Consider the matrices of the form

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ 0 & 0 & \cdots & * \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

They form a subgroup H of order $p^{n-1}p^{n-2}\cdots p$, which is therefore a Sylow p-subgroup G.

Corollary 5.6. *Any group of order $2p$, p an odd prime, is cyclic or dihedral.*

Proof. From the last corollary, we know that such a G contains elements τ and σ of orders 2 and p respectively. Let $H = <\sigma>$. Then H is of index 2, and so is normal. Obviously $\tau \notin H$, and so $G = H \cup H\tau$:

$$G = \{1, \sigma, \ldots, \sigma^{p-1}, \tau, \sigma\tau, \ldots, \sigma^{p-1}\tau\}.$$

As H is normal, $\tau\sigma\tau^{-1} = \sigma^i$, some i. Because $\tau^2 = 1$, $\sigma = \tau^2\sigma\tau^{-2} = \tau(\tau\sigma\tau^{-1})\tau^{-1} = \sigma^{i^2}$, and so $i^2 \equiv 1 \bmod p$. The only elements of $\mathbb{F}_p$ with square 1 are ± 1, and so $i \equiv 1$ or -1 mod p. In the first case, the group is commutative (any group generated by a set of commuting elements is obviously commutative); in the second $\tau\sigma\tau^{-1} = \sigma^{-1}$ and we have the dihedral group. □

Theorem 5.7 (Sylow II). *Let G be a finite group, and let $(G:1) = p^r m$ with m not divisible by p.*

(a) *Any two Sylow p-subgroups are conjugate.*
(b) *Let s_p be the number of Sylow p-subgroups in G; then $s_p | m$, and $s_p \equiv 1 \bmod p$.*
(c) *Any p-subgroup of G is contained in a Sylow p-subgroup.*

Let H be a subgroup of G. Recall (p27) that the normalizer of H in G is

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\},$$

and that the number of conjugates of H in G is $(G : N_G(H))$. For a Sylow p-subgroup P, the number of conjugates of P is

$$(G : N_G(P)) = \frac{(G:1)}{(N_G(P):1)} = \frac{(G:1)}{(N_G(P):P)\cdot(P:1)} = \frac{m}{(N_G(P):P)}.$$

Thus (a) of the theorem implies that $s_p = (G : N_G(P))$, which, we have just seen, divides m. In order to prove the rest of the theorem, we need the following key lemma.

Lemma 5.8. *Let P be a Sylow p-subgroup of G, and let H be a p-subgroup. If H normalizes P, i.e., if $H \subset N_G(P)$, then $H \subset P$. Therefore no Sylow p-subgroup of G other than P normalizes P.*

Proof. Because H and P are subgroups of $N_G(P)$ with P normal in $N_G(P)$, HP is a subgroup, and $H/H \cap P \approx HP/P$ (see 3.2). Therefore $(HP : P)$ is a power of p (here is where we use that H is a p-group), but

$$(HP : 1) = (HP : P)(P : 1),$$

and $(P : 1)$ is the largest power of p dividing $(G : 1)$, hence also the largest power of p dividing $(HP : 1)$. Thus $(HP : P) = p^0 = 1$, and $H \subset P$. □

Proof. (of Sylow II). This time we let $X = \{\text{Sylow } p\text{-subgroups}\}$, and we let G act on X by conjugation. Let O be one of the G-orbits: we have to show O is all of X.

Let $P \in O$, and consider the action by conjugation of P on O. This single G-orbit may break up into several P-orbits, one of which will be $\{P\}$. In fact this is the only one-point orbit because $\{Q\}$ is a P-orbit if and only if P normalizes Q, but we know from Lemma 5.8 that then $Q = P$. Hence the number of elements in every P-orbit other than $\{P\}$ is divisible by p, and we have that $\#O \equiv 1 \bmod p$.

Suppose there is a $P \notin O$. We again let P act on O, but this time the argument shows that there are no one-point orbits, and so the number of elements in every P-orbit is divisible by p. This implies that $\#O$ is divisible by p, which contradicts what we proved in the last paragraph. There can be no such P, and so O is all of X—we have proved (a).

Since s_p is now the number of elements in O, we have also shown that $s_p \equiv 1 \pmod p$, and so it remains to prove (c).

Let H be a p-subgroup of G, and let H act on the set X of Sylow p-subgroups by conjugation. Because $\#X = s_p$ is not divisible by p, X^H must be nonempty (Lemma 5.1), i.e., at least one H-orbit consists of a single Sylow p-subgroup. But then H normalizes P and Lemma 5.8 implies that $H \subset P$. □

Corollary 5.9. *A Sylow p-subgroup is normal $\iff$ it is the only Sylow p-subgroup.*

Proof. In fact (without using the Sylow theorems), we know (3.12c) that if P is the only Sylow p-subgroup, then P is characteristic. The converse follows from (a) of Sylow II. □

Corollary 5.10. *Suppose that a group G has only one Sylow p-subgroup for each $p|(G : 1)$. Then G is a product of its Sylow p-subgroups.*

Proof. Let $P_1, \dots, P_r$ be the Sylow subgroups of G. Because they are normal, P_1P_2 is a normal subgroup of G. Moreover $P_1 \cap P_2 = 1$, and so (3.6) implies $(a,b) \mapsto ab : P_1 \times P_2 \to P_1P_2$ is an isomorphism (cf. Exercise 15). In particular, P_1P_2 has order $p_1^{n_1}p_2^{n_2}$ where $p_i^{n_i} = (P_i : 1)$. Now $P_1P_2 \cap P_3 = 1$, and so $P_1 \times P_2 \times P_3 \approx P_1P_2P_3$. Continue in this manner. □

Example 5.11. There is a geometric description of the Sylow subgroups of $G = \mathrm{GL}_n(\mathbb{F}_p)$. Let $V = \mathbb{F}_p^n$, regarded as a vector space of dimension n over $\mathbb{F}_p$. A *full flag* F in V is a sequence of subspaces

$$V = V_n \supset V_{n-1} \supset \cdots \supset V_i \supset \cdots \supset V_1 \supset \{0\}$$

with $\dim V_i = i$. Given such a flag F_0, let $P(F_0)$ be the set of linear maps $\alpha : V \to V$ such that

(a) $\alpha(V_i) \subset V_i$ for all i, and
(b) the endomorphism of V_i/V_{i-1} induced by α is the identity map.

I claim that $P(F_0)$ is a Sylow p-subgroup of G. Indeed, we can construct a basis $\{e_1, \dots, e_n\}$ for V such $\{e_1\}$ is basis for V_1, $\{e_1, e_2\}$ is a basis for V_2, etc.. Relative to this basis, the matrices of the elements of $P(F_0)$ are exactly the elements of the group P of (5.5).

Let $\alpha \in \mathrm{GL}_n(\mathbb{F})$. Then $\alpha F_0 =_{df} \{\alpha V_n, \alpha V_{n-1}, \dots\}$ is again a full flag, and $P(\alpha F_0) = \alpha P(F_0)\alpha^{-1}$. From (a) of Sylow II, we see that the Sylow p-subgroups of G are precisely the groups of the form $P(F)$ for some full flag F.

5.2. Classification.

We apply what we have learnt to obtain information about groups of various orders.

Example 5.12 (Groups of order 99). Let G have order 99. The Sylow theorems imply that G has at least one subgroup H of order 11, and in fact $s_{11} \Big| \frac{99}{11}$ and $s_{11} \equiv 1 \mod 11$. It follows that $s_{11} = 1$, and H is normal. Similarly, $s_9 | 11$ and $s_9 \equiv 1 \mod 3$, and so the Sylow 3-subgroup is also normal. Hence G is isomorphic to the product of its Sylow subgroups, and so is commutative.

Here is an alternative proof. Verify as before that the Sylow 11-subgroup N of G is normal. The Sylow 3-subgroup Q maps bijectively onto G/N, and so $G = N \rtimes Q$. It remains to determine the action by conjugation of Q on N. But $\mathrm{Aut}(N)$ is cyclic of order 10 (see 3.9, 3.10), and so the only homomorphism $Q \to \mathrm{Aut}(N)$ is the trivial one (the homomorphism that maps everything to 1). It follows that G is commutative.

Example 5.13 (Groups of order pq, p, q primes, $p < q$). Let G be such a group, and let P and Q be Sylow p and q subgroups. Then $(G : Q) = p$, which is the smallest prime dividing $(G : 1)$, and so (see Exercise 22) Q is normal. Because P maps bijectively onto G/Q, we have that

$$G = Q \rtimes P,$$

and it remains to determine the action of P on Q by conjugation.

The group $\mathrm{Aut}(Q)$ is cyclic of order $q-1$, and so, unless $p | q-1$, $G = Q \times P$.

If $p | q-1$, then $\mathrm{Aut}(Q)$ (being cyclic) has a unique subgroup P' of order p. In fact P' consists of the maps

$$x \mapsto x^i, \quad \{i \in \mathbb{F}_q \mid i^p = 1\}.$$

Let a and b be generators for P and Q respectively, and suppose that the action of a on Q by conjugation is $x \mapsto x^{i_0}$, $i_0 \neq 1$ (in $\mathbb{F}_q$). Then G has generators a, b and relations a^p, b^q, $aba^{-1} = b^{i_0}$. Choosing a different i_0 amounts to choosing a different generator a for P, and so gives an isomorphic group G.

In summary: if $p \nmid q-1$, then the only group of order pq is the cyclic group C_{pq}; if $p|q-1$, then there is also a nonabelian group given by the above generators and relations.

The semidirect product $N \rtimes_\theta Q$ is determined by the triple $(N, Q, \theta : Q \to \mathrm{Aut}(N))$. It will be useful to have criteria for when two triples (N, Q, θ) and (N, Q, θ') determine isomorphic groups.

Lemma 5.14. *If θ and θ' are conjugate, i.e., there exists an $\alpha \in \mathrm{Aut}(N)$ such that $\theta' = \alpha \circ \theta(q) \circ \alpha^{-1}$ for all $q \in Q$, then*

$$N \rtimes_\theta Q \approx N \rtimes_{\theta'} Q.$$

Proof. Consider the map

$$\gamma : N \rtimes_\theta Q \to N \rtimes_{\theta'} Q, \quad (n, q) \mapsto (\alpha(n), q).$$

Then

$$\gamma(n, q) \cdot \gamma(n', q') = (\alpha(n), q) \cdot (\alpha(n'), q') = (\alpha(n) \cdot (\alpha \circ \theta(q) \circ \alpha^{-1})(\alpha(n')), qq'),$$

and

$$\gamma((n, q) \cdot (n', q')) = \gamma(n \cdot \theta(q)(n'), qq') = (\alpha(n) \cdot (\alpha \circ \theta)(q)(n'), qq').$$

Therefore γ is a homomorphism, with inverse $(n, q) \mapsto (\alpha^{-1}(n), q)$, and so is an isomorphism. □

Lemma 5.15. *If $\theta = \theta' \circ \alpha$ with $\alpha \in \mathrm{Aut}(Q)$, then*

$$N \rtimes_\theta Q \approx N \rtimes_{\theta'} Q.$$

Proof. The map $(n, q) \mapsto (n, \alpha(q))$ is an isomorphism $N \rtimes_\theta Q \to N \rtimes_{\theta'} Q$. □

Lemma 5.16. *If Q is cyclic and the subgroup $\theta(Q)$ of $\mathrm{Aut}(N)$ is conjugate to $\theta'(Q)$, then*

$$N \rtimes_\theta Q \approx N \rtimes_{\theta'} Q.$$

Proof. Let a generate Q. Then there exists an i and an $\alpha \in \mathrm{Aut}(N)$ such that

$$\theta'(a^i) = \alpha \cdot \theta(a) \cdot \alpha^{-1}.$$

The map $(n, q) \mapsto (\alpha(n), q^i)$ is an isomorphism $N \rtimes_\theta Q \to N \rtimes_{\theta'} Q$. □

Example 5.17 (Groups of order 30). Let G be a group of order 30. Then

$$\begin{aligned} s_3 &= 1, 4, 7, 10, \ldots \text{ and divides } 10; \\ s_5 &= 1, 6, 11, \ldots \text{ and divides } 6. \end{aligned}$$

Hence $s_3 = 1$ or 10, and $s_5 = 1$ or 6. In fact, at least one is 1, for otherwise there would be 20 elements of order 2 and 24 elements of order 5, which is impossible. Therefore, a Sylow 3-subgroup P or a Sylow 5-subgroup Q is normal, and so $H = PQ$ is a subgroup of G. Because 3 doesn't divide $5 - 1 = 4$, (5.13) shows that H is commutative, $H \approx C_3 \times C_5$. Hence

$$G = (C_3 \times C_5) \rtimes_\theta C_2,$$

and it remains to determine the possible homomorphisms $\theta : C_2 \to \mathrm{Aut}(C_3 \times C_5)$. But such a homomorphism θ is determined by the image of the nonidentity element of C_2, which must be an element of order 2. Let a, b, c generate C_3, C_5, C_2. Then

$$\mathrm{Aut}(C_3 \times C_5) = \mathrm{Aut}(C_3) \times \mathrm{Aut}(C_5),$$

and the only nontrivial elements of $\mathrm{Aut}\, C_3$ and $\mathrm{Aut}\, C_5$ are $a \mapsto a^{-1}$ and $b \mapsto b^{-1}$. Thus there are exactly 4 homomorphisms θ, and $\theta(c)$ is one of the following elements:

$$\left\{\begin{array}{c} a \mapsto a \\ b \mapsto b \end{array}\right. \quad \left\{\begin{array}{c} a \mapsto a \\ b \mapsto b^{-1} \end{array}\right. \quad \left\{\begin{array}{c} a \mapsto a^{-1} \\ b \mapsto b \end{array}\right. \quad \left\{\begin{array}{c} a \mapsto a^{-1} \\ b \mapsto b^{-1} \end{array}\right. .$$

The groups corresponding to these homomorphisms have centres of order 30, 3 (generated by a), 5 (generated by b), and 1 respectively, and hence are nonisomorphic. We have shown that (up to isomorphism) there are exactly 4 groups of order 30. For example, the third on our list has generators a, b, c and relations

$$a^3, \quad b^5, \quad c^2, \quad ab = ba, \quad cac^{-1} = a^{-1}, \quad cbc^{-1} = b.$$

Example 5.18 (Groups of order 12). Let G be a group of order 12, and let P be its Sylow 3-subgroup. If P is not normal, then the map (4.2c)

$$\varphi : G \to \mathrm{Sym}(G/P) \approx S_4$$

is injective, and its image is a subgroup of S_4 of order 12. From Sylow II we see that G has exactly 4 Sylow 3-subgroups, and hence it has exactly 8 elements of order 3. But all elements of S_4 of order 3 are in A_4 (see 4.27), and so $\varphi(G)$ intersects A_4 in a subgroup with at least 8 elements. By Lagrange's theorem $\varphi(G) = A_4$, and so $G \approx A_4$.

Thus, assume P is normal. Then $G = P \rtimes Q$ where Q is the Sylow 4-subgroup. If Q is cyclic of order 4, then there is a unique nontrivial map $Q(= C_4) \to \mathrm{Aut}(P)(= C_2)$, and hence we obtain a single noncommutative group $C_3 \rtimes C_4$. If $Q = C_2 \times C_2$, there are exactly 3 nontrivial homomorphism $\theta : Q \to \mathrm{Aut}(P)$, but the three groups resulting are all isomorphic to $S_3 \times C_2$ with $C_2 = \mathrm{Ker}\,\theta$. (The homomorphisms differ by an automorphism of Q, and so we can also apply Lemma 5.15.)

In total, there are 3 noncommutative groups of order 12 and 2 commutative groups

Example 5.19 (Groups of order p^3). Let G be a group of order p^3, with p an odd prime, and assume G is not commutative. We know from (4.15) that G has a normal subgroup N of order p^2.

If every element of G has order p (except 1), then $N \approx C_p \times C_p$ and there is a subgroup Q of G of order p such that $Q \cap N = \{1\}$. Hence

$$G = N \rtimes_\theta Q$$

for some homomorphism $\theta : Q \to N$. The Sylow p-subgroups of N have order p (special case of 5.5), and so we can apply Lemma 5.16 to see that there we obtain only one nonabelian group in this case.

Suppose G has elements of order p^2, and let N be the subgroup generated by such an element a. Because $(G : N) = p$ is the smallest (in fact only) prime dividing $(G : 1)$, N is normal in G. The problem is to show that G contains an element of order p not in N.

We know $Z(G) \neq 1$, and (see 4.17) that $G/Z(G)$ is not cyclic. Therefore $(Z(G) : 1) = p$ and $G/Z(G) \approx C_p \times C_p$. In particular, we see that for all $x \in G$, $x^p \in Z(G)$. Because $G/Z(G)$

is commutative, the commutator $[x, y] \in Z(G)$ for all $x, y \in G$, and an easy induction argument shows that

$$(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}, \quad n \geq 1.$$

Therefore $(xy)^p = x^p y^p$, and so $x \mapsto x^p : G \to G$ is a homomorphism. Its image is contained in $Z(G)$, and so its kernel has order at least p^2. Since N contains only $p-1$ elements of order p, we see that there exists an element b outside N. Hence $G = <a> \rtimes <b> \approx C_{p^2} \rtimes C_p$, and it remains to observe (5.16) that the nontrivial homomorphisms $C_p \to \text{Aut}(C_{p^2}) \approx C_p \times C_{p-1}$ give isomorphic groups.

Thus, up to isomorphism, the only noncommutative groups of order p^3 are those constructed in (3.16e).

Example 5.20 (Groups of order $2^m p^n$, p odd). Let G be a group of order $2^m p^n$, $1 \leq m \leq 3$, p an odd prime, $1 \leq n$. We shall show that G is not simple. Let P be a Sylow p-subgroup and let $N = N_G(P)$, so that $s_p = (G : N)$.

From Sylow II, we know that $s_p | 2^m$, $s_p = 1, p+1, \ldots$. If $s_p = 1$, P is normal. If not, there are two cases to consider:

(i) $s_p = 4$ and $p = 3$, or
(ii) $s_p = 8$ and $p = 7$.

In the first case, the action by conjugation of G on the set of Sylow 3-subgroups[12] defines a homomorphism $G \to S_4$, which, if G is simple, must be injective. Therefore $(G : 1)|4!$, and so $n = 1$; we have $(G : 1) = 2^m 3$. Now the Sylow 2-subgroup has index 3, and we have a homomorphism $G \to S_3$. Its kernel is a nontrivial normal subgroup of G.

In the second case, the same argument shows that $(G : 1)|8!$, and so $n = 1$ again. Thus $(G : 1) = 56$ and $s_7 = 8$. Therefore G has 48 elements of order 7, and so there can be only one Sylow 2-subgroup, which must therefore be normal.

Note that groups of order pq^r, p, q primes, $p < q$ are not simple, because Exercise 22 shows that the Sylow q-subgroup is normal. An examination of cases now reveals that A_5 is the smallest noncyclic simple group.

Example 5.21. Let G be a simple group of order 60. We shall show that G is isomorphic to A_5.

Note that, because G is simple, $s_2 = 3, 5$, or 15. If P is a Sylow 2-subgroup and $N = N_G(P)$, then $s_2 = (G : N)$.

The case $s_2 = 3$ is impossible, because the kernel of $G \to \text{Sym}(G/N)$ would be a nontrivial subgroup of G.

In the case $s_2 = 5$, we get an inclusion $G \hookrightarrow \text{Sym}(G/N) = S_5$, which realizes G as a subgroup of index 2 in S_5, but we saw in (4.32) that A_n is the only subgroup of index 2 in S_5.

In the case $s_2 = 15$, a counting argument (using that $s_5 = 6$) shows that there exist two Sylow 2-subgroups P and Q intersecting in a group of order 2. The normalizer N of $P \cap Q$ contains P and Q, and so has order 12, 20, or 60. In the first case, the above argument show that $G \approx A_5$, and the remaining cases contradict the simplicity of G.

[12] Equivalently, the usual map $G \to \text{Sym}(G/N)$.

6. Normal Series; Solvable and Nilpotent Groups

6.1. Normal Series.

Let G be a group. A *normal series* (better *subnormal series*) in G is a finite chain of subgroups

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_i \rhd G_{i+1} \rhd \cdots \rhd G_n = \{1\}.$$

Thus G_{i+1} is normal in G_i, but not necessarily in G. The series is said to be without repetitions if $G_i \neq G_{i+1}$. Then n is called the *length* of the series. The quotient groups G_i/G_{i+1} are called the *quotient* (or *factor)* groups of the series.

A normal series is said to be a *composition series* if it has no repetitions and can't be refined, i.e., if G_{i+1} is a maximal proper subgroup in G_i for each i. Thus a normal series is a composition series $\iff$ each quotient group is simple and $\neq 1$. Obviously, every finite group has a composition series (usually many): choose G_1 to be a maximal proper normal subgroup of G; then choose G_2 to be a maximal proper normal subgroup of G_1, etc.. An infinite group may or may not have a finite composition series.

Note that from a normal series

$$G = G_n \rhd G_{n-1} \rhd \cdots \rhd G_{i+1} \rhd G_i \rhd \cdots \rhd G_1 \supset \{1\}$$

we obtain a sequence of exact sequences

$$1 \to G_1 \to G_2 \to G_2/G_1 \to 1$$

$$1 \to G_2 \to G_3 \to G_3/G_2 \to 1$$

$$\cdots$$

$$1 \to G_{n-1} \to G_n \to G_n/G_{n-1} \to 1.$$

Thus G is built up out of the quotients $G_1, G_2/G_1, \ldots, G_n/G_{n-1}$ by forming successive extensions. In particular, since every finite group has a composition series, it can be regarded as being built up out of simple groups. The Jordan-Hölder theorem says that these simple groups are (essentially) independent of the composition series.

Note that if G has a normal series $G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots$, then

$$(G:1) = \prod (G_{i-1} : G_i) = \prod (G_{i-1}/G_i : 1).$$

Example 6.1. (a) The symmetric group S_3 has a composition series

$$S_3 \rhd A_3 \rhd 1$$

with quotients C_2, C_3.

(b) The symmetric group S_4 has a composition series

$$S_4 \rhd A_4 \rhd V \rhd <(13)(24)> \rhd 1,$$

where $V \approx C_2 \times C_2$ consists of all elements of order 2 in A_4 (see 4.27). The quotients are C_2, C_3, C_2, C_2.

(c) Any full flag in $\mathbb{F}_p^n$, p a prime, is a composition series. Its length is n, and its quotients are $C_p, C_p, \ldots, C_p$.

(d) Consider the cyclic group C_m. For any factorization $m = p_1 \cdots p_r$ of m into a product of primes, there is a composition series

$$\begin{tikzcd}
C_m \arrow[r, phantom, "\triangleright"] \arrow[d, equal] & C_{\frac{m}{p_1}} \arrow[r, phantom, "\triangleright"] \arrow[d, equal] & C_{\frac{m}{p_1 p_2}} \arrow[r, phantom, "\triangleright"] \arrow[d, equal] & \cdots \\
<\sigma> & <\sigma^{p_1}> & <\sigma^{p_1 p_2}> &
\end{tikzcd}$$

The length is r, and the quotients are $C_{p_1}, C_{p_2}, \ldots, C_{p_r}$.

(e) Suppose G is a product of simple groups, $G = H_1 \times \cdots \times H_r$. Then G has a composition series

$$G \triangleright H_2 \times \cdots \times H_r \triangleright H_3 \times \cdots \times H_r \triangleright \cdots$$

of length r and with quotients $H_1, H_2, \ldots, H_r$. Note that for any permutation π of $\{1, 2, \ldots r\}$, there is another composition series with quotients $H_{\pi(1)}, H_{\pi(2)}, \ldots, H_{\pi(r)}$.

(f) We saw in (4.32) that for $n \geq 5$, the only normal subgroups of S_n are S_n, A_n, $\{1\}$, and in (4.28) that A_n is simple. Hence $S_n \triangleright A_n \triangleright \{1\}$ is the *only* composition series for S_n.

As we have seen, a finite group may have many composition series. The Jordan-Hölder theorem says that they all have the same length, and the same quotients (up to order and isomorphism). More precisely:

Theorem 6.2 (Jordan-Hölder). *If*

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_s = \{1\}$$

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_t = \{1\}$$

are two composition series for G, then $s = t$ and there is a permutation π of $\{1, 2, \ldots, s\}$ such that $G_i/G_{i+1} \approx H_{\pi(i)}/H_{\pi(i+1)}$. [13]

Proof. We use induction on the order of G.

Case I: $H_1 = G_1$. In this case, we have two composition series for G_1, to which we can apply the induction hypothesis.

Case II: $H_1 \neq G_1$. Because each of G_1 and H_1 is normal in G, $G_1 H_1$ is a normal subgroup of G, and it properly contains both G_1 and H_1. But they are maximal normal subgroups of G, and so $G_1 H_1 = G$. Therefore

$$G/G_1 = G_1 H_1/G_1 \approx H_1/G_1 \cap H_1 \qquad \text{(see 3.2).}$$

Similarly $G/H_1 \approx G_1/G_1 \cap H_1$. Hence $K_2 =_{df} G_1 \cap H_1$ is a maximal normal subgroup in both G_1 and H_1, and

$$G/G_1 \approx H_1/K_2, \quad G/H_1 \approx G_1/K_2.$$

Choose a composition series

$$K_2 \triangleright K_3 \triangleright \cdots \triangleright K_u.$$

We have the picture:

$$\begin{tikzcd}
 & G_1 \arrow[r, phantom, "\triangleright"] \arrow[dr, dash] & G_2 \arrow[r, phantom, "\triangleright"] & \cdots \arrow[r, phantom, "\triangleright"] & G_s \\
G \arrow[ur, dash] \arrow[dr, dash] & & K_2 \arrow[r, phantom, "\triangleright"] & \cdots \arrow[r, phantom, "\triangleright"] & K_u & . \\
 & H_1 \arrow[r, phantom, "\triangleright"] \arrow[ur, dash] & H_2 \arrow[r, phantom, "\triangleright"] & \cdots \arrow[r, phantom, "\triangleright"] & H_t
\end{tikzcd}$$

[13] Jordan showed that corresponding quotients had the same order, and Hölder that they were isomorphic.

On applying the induction hypothesis to G_1 and H_1 and their composition series in the diagram, we find that

$$\begin{aligned}\text{Quotients}(G \rhd G_1 \rhd G_2 \rhd \cdots) &\sim \{G/G_1, G_1/G_2, G_2/G_3, \dots\}\\ &\sim \{G/G_1, G_1/K_2, K_2/K_3, \dots\}\\ &\sim \{H_1/K_2, G/H_1, K_2/K_3, \dots\}\\ &\sim \{G/H_1, H_1/H_2, H_2/H_3, \dots\}\\ &\sim \text{Quotients}(G \rhd H_1 \rhd H_2 \rhd \cdots).\end{aligned}$$

In passing from the second to the third line, we used the isomorphisms $G/G_1 \approx H_1/K_2$ and $G/H_1 \approx G_1/K_2$. □

Note that the theorem applied to a cyclic group C_m implies that the factorization of an integer into a product of primes is unique.

Remark 6.3. There are infinite groups having finite composition series (there are infinite simple groups). For such a group, let $d(G)$ be the minimum length of a composition series. Then the Jordan-Hölder theorem extends to show that all composition series have length $d(G)$ and have isomorphic quotient groups. The same proof works: use induction on $d(G)$ instead of $(G : 1)$.

The quotients of a composition series are also called *composition factors.* (Some authors call a quotient group G/N a "factor" group of G; I prefer to reserve this term for a subgroup H of G such that $G = H \times H'$.)

6.2. Solvable groups.

A group is *solvable* if it has a normal series whose quotient groups are all commutative. Such a series is called a *solvable series.* Alternatively, we can say that a group is solvable if it can be obtained by forming successive extensions of abelian groups. Since a commutative group is simple if and only if it is cyclic of prime order, we see that G is solvable if and only if for one (hence every) composition series the quotients are all cyclic groups of prime order.

Any commutative group is solvable, as is any dihedral group. The results in Section 5 show that every group of order < 60 is solvable. By contrast, a noncommutative simple group, e.g., A_n for $n \geq 5$, will not be solvable.

There is the following result:

Theorem 6.4 (Feit-Thompson 1963). *Every finite group of odd order is solvable.*

Proof. The proof occupies a whole issue of the Pacific J. Math., and hence is omitted. □

This theorem played a very important role in the development of group theory, because it shows that every noncommutative finite simple group contains an element of order 2. It was a starting point in the program that eventually led to the classification of all finite simple groups.

Example 6.5. Consider the subgroups $G = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}$ and $G_1 = \left\{\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\right\}$ of $\mathrm{GL}_2(k)$, some field k. Then G_1 is a normal subgroup of G, and $G/G_1 \approx k^\times \times k^\times$, $G_1 \approx (k, +)$. Hence G is solvable.

Proposition 6.6. *(a) Every subgroup and every quotient group of a solvable group is solvable.*

(b) An extension of solvable groups is solvable.

Proof. (a) Let $G \rhd G_1 \rhd \cdots \rhd G_n$ be a solvable series for G, and let H be a subgroup of G. The homomorphism

$$x \mapsto xG_{i+1} : H \cap G_i \to G_i/G_{i+1}$$

has kernel $(H \cap G_i) \cap G_{i+1} = H \cap G_{i+1}$. Therefore $H \cap G_{i+1}$ is a normal subgroup of $H \cap G_i$ and the quotient $H \cap G_i/H \cap G_{i+1}$ injects into G_i/G_{i+1}, and so is commutative. We have shown that

$$H \rhd H \cap G_1 \rhd \cdots \rhd H \cap G_n$$

is a solvable series for H.

Let $\bar{G}$ be a quotient group of G, and let $\bar{G}_i$ be the image of G_i in $\bar{G}$. Then

$$\bar{G} \rhd \bar{G}_1 \rhd \cdots \rhd \bar{G}_n = \{1\}$$

is a solvable series for $\bar{G}$.

(b) Let N be a normal subgroup of G, and let $\bar{G} = G/N$. We have to show that if N and $\bar{G}$ are solvable, then so also is G. Let

$$\bar{G} \rhd \bar{G}_1 \rhd \cdots \rhd \bar{G}_n = \{1\}$$

$$N \rhd N_1 \rhd \cdots \rhd N_m = \{1\}$$

be a solvable series for $\bar{G}$ and N, and let G_i be the inverse image of $\bar{G}_i$ in G. Then $G_i/G_{i+1} \approx \bar{G}_i/\bar{G}_{i+1}$ (see 3.4), and so the

$$G \rhd G_1 \rhd \cdots \rhd G_n(= N) \rhd N_1 \rhd \cdots \rhd N_m$$

is a solvable series for G. □

Corollary 6.7. *A finite p-group is solvable.*

Proof. We use induction on the order the group G. According to (4.14), the centre $Z(G)$ of G is nontrivial, and so the induction hypothesis shows that $G/Z(G)$ is solvable. Because $Z(G)$ is solvable, Proposition 6.6b shows that G is solvable. □

Let G be a group. Recall that the commutator of $x, y \in G$ is

$$[x, y] = xyx^{-1}y^{-1} = xy(yx)^{-1}$$

Thus $[x, y] = 1 \iff xy = yx$, and G is commutative $\iff$ all commutators are 1.

Example 6.8. For any finite-dimensional vector space V over a field k and any full flag $F = \{V_n, V_{n-1}, \ldots\}$ in V, the group

$$B(F) = \{\alpha \in \mathrm{Aut}(V) \mid \alpha(V_i) \subset V_i \text{ all } i\}$$

is solvable. When $k = \mathbb{F}_p$, this can be proved by noting that $B(F)/P(F)$ is commutative, and that $P(F)$ is a p-group and is therefore solvable. The general case is left as an exercise.

For any homomorphism $\varphi : G \to H$

$$\varphi[x,y] = \varphi(xyx^{-1}y^{-1}) = [\varphi(x), \varphi(y)]$$

i.e., φ maps the commutator of x, y to the commutator of $\varphi(x), \varphi(y)$. In particular, we see that if H is commutative, then φ maps all commutators in G to 1.

The group G' generated by the commutators in G is called the *commutator* or *first derived* subgroup of G.

Proposition 6.9. *The commutator subgroup G' is a characteristic subgroup of G; it is the smallest normal subgroup of G such that G/G' is commutative.*

Proof. An automorphism α of G maps the generating set for G' into G', and hence maps G' into G'. Since this is true for all automorphisms of G, G' is characteristic.

Write $g \mapsto \bar{g}$ for the map $g \mapsto gG' : G \to G/G'$; then $[g,h] \mapsto [\bar{g}, \bar{h}]$; but $[g,h] \mapsto 1$ and so $[\bar{g}, \bar{h}] = 1$ for all $\bar{g}$, $\bar{h} \in G/G'$. Hence G/G' is commutative.

If N is normal and G/N is commutative, then $[g,h] \mapsto 1$ in G/N, and so $[g,h] \in N$. Since these elements generate G', $N \supset G'$. □

For $n \geq 5$, A_n is the smallest normal subgroup of S_n giving a commutative quotient. Hence $(S_n)' = A_n$.

The *second derived* subgroup of G is $(G')'$; the *third* is $G^{(3)} = (G'')'$; and so on. Each derived group is a characteristic subgroup of G. Hence we obtain a normal series

$$G \supset G' \supset G^{(2)} \supset \cdots,$$

which is called the *derived series.* For example, if $n \geq 5$, then the derived series of S_n is

$$S_n \supset A_n \supset A_n \supset A_n \supset \cdots.$$

Proposition 6.10. *A group G is solvable if and only if its k^{th} derived subgroup $G^{(k)} = 1$ for some k.*

Proof. If $G^{(k)} = 1$, then the derived series is a solvable series for G. Conversely, let

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s = \{0\}$$

be a solvable series for G. Because G/G_1 is commutative, $G_1 \supset G'$. Now $G'G_2$ is a subgroup of G_1, and from

$$G'/G' \cap G_2 \xrightarrow{\approx} G'G_2/G_2 \subset G_1/G_2$$

we see that

$$G_1/G_2 \text{ commutate } \implies G'/G' \cap G_2 \text{ commutative } \implies G'' \subset G' \cap G_2 \subset G_2.$$

On continuing in the fashion, we find that $G^{(i)} \subset G_i$ for all i, and hence $G^{(s)} = 1$. □

Thus, a solvable group G has a *canonical* solvable series, namely the derived series, in which all the groups are normal in G. The derived series is the shortest solvable series for G. Its length is called the *solvable length* of G.

6.3. Nilpotent groups.

Let G be a group. Recall that we write $Z(G)$ for the centre of G. Let $Z^2(G) \supset Z(G)$ be the subgroup of G corresponding to $Z(G/Z(G))$. Thus

$$g \in Z^2(G) \iff [g,x] \in Z(G) \text{ for all } x \in G.$$

Continuing in this fashion, we get a sequence of subgroups (*ascending central series*)

$$\{1\} \subset Z(G) \subset Z^2(G) \subset \cdots$$

where $g \in Z^i(G) \iff [g,x] \in Z^{i-1}(G)$ for all $x \in G$. If $Z^m(G) = G$ for some m, then G is said to be *nilpotent*, and the smallest such m is called the *(nilpotency) class* of G. For example, all finite p-groups are nilpotent.

For example, only the group $\{1\}$ has nilpotency class 0, and only the abelian groups have class 1. A group G is of class 2 if and only if $G/Z(G)$ is commutative—such a group is said to be *metabelian*.

Example 6.11. (a) Nilpotent $\implies$ solvable, but not conversely. For example, for a field k, let

$$G = \left\{ \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \middle| a,b,c \in k, \quad ac \neq 0 \right\}.$$

Then $Z(G) = \{aI \mid a \neq 0\}$, and the centre of $G/Z(G)$ is trivial. Therefore $G/Z(G)$ is not nilpotent, but it is solvable.

(b) The group $G = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}$ is metabelian: its centre is $\left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$, and $G/Z(G)$ is commutative.

(c) Any nonabelian group G of order p^3 is metabelian. In fact, $G' = Z(G)$, which has order p (see 5.21).

(d) The quaternion and dihedral groups of order 8, Q and D_4, are nilpotent of class 2. More generally, D_{2^n} is nilpotent of class n—this can be proved by induction, using that $Z(D_{2^n})$ has order 2, and $D_{2^n}/Z(D_{2^n}) \approx D_{2^{n-1}}$. If n is not a power of 2, then D_n is not nilpotent (use Theorem 6.17).

Proposition 6.12. *(a) A subgroup of a nilpotent group is nilpotent.*

(b) A quotient of a nilpotent group is nilpotent.

Proof. (a) Let H be a subgroup of a nilpotent group G. Clearly, $Z(H) \supset Z(G) \cap H$. Assume (inductively) that $Z^i(H) \supset Z^i(G) \cap H$; then $Z^{i+1}(H) \supset Z^{i+1}(G) \cap H$, because (for $h \in H$)

$$h \in Z^{i+1}(G) \implies [h,x] \in Z^i(G) \text{ all } x \in G \implies [h,x] \in Z^i(H) \text{ all } x \in H.$$

(b) Straightforward. □

Remark 6.13. It is worth noting that if H is a subgroup of G, then $Z(H)$ may be bigger than $Z(G)$. For example

$$H = \left\{ \left(\begin{array}{cc} a & 0 \\ 0 & b \end{array} \right) \middle| ab \neq 0 \right\} \subset \mathrm{GL}_2(k).$$

is commutative, i.e., $Z(H) = H$, but the centre of G consists of only of the scalar matrices.

Proposition 6.14. *A group G is nilpotent of class $\leq m \iff [...[[g_1, g_2], g_3], ..., g_{m+1}] = 1$ for all $g_1, ..., g_{m+1} \in G$.*

Proof. Recall, $g \in Z^i(G) \iff [g, x] \in Z^{i-1}(G)$ for all $x \in G$.

Assume G is nilpotent of class $\leq m$; then

$$\begin{aligned} G = Z^m(G) \quad &\implies \quad [g_1, g_2] \in Z^{m-1}(G) \text{ all } g_1, g_2 \in G \\ &\implies \quad [[g_1, g_2], g_3] \in Z^{m-2}(G) \text{ all } g_1, g_2, g_3 \in G \\ \cdots\cdots & \\ &\implies \quad [\cdots[[g_1, g_2], g_3], ..., g_m] \in Z(G) \text{ all } g_1, \ldots, g_m \in G \\ &\implies \quad [\cdots[[g_1, g_2], g_3], \ldots, g_{m+1}] = 1 \text{ all } g_1, \ldots, g_m \in G. \end{aligned}$$

For the converse, let $g_1 \in G$. Then

$$[...[[g_1, g_2], g_3], ..., g_m], g_{m+1}] = 1 \text{ for all } g_1, g_2, ..., g_{m+1} \in G$$

$$\begin{aligned} &\implies \quad [...[[g_1, g_2], g_3], ..., g_m] \in Z(G), \text{ for all } g_1, ..., g_m \in G \\ &\implies \quad [...[[g_1, g_2], g_3], ..., g_{m-1}] \in Z^1(G), \text{ for all } g_1, ..., g_{m-1} \in G \\ &\implies \quad g_1 \in Z^m(G) \text{ all } g_1 \in G. \end{aligned}$$

□

It is not true that an extension of nilpotent groups is nilpotent, i.e.,

$$N \text{ and } G/N \text{ nilpotent } \not\Rightarrow G \text{ nilpotent.}$$

For example, the subgroup N of the group G in (6.11) is commutative and G/N is commutative, but G is not nilpotent. However, the implication holds when N is contained in the centre of G

Corollary 6.15. *Consider $N \subset Z(G)$; G/N nilpotent of class $m \implies G$ nilpotent of class $\leq m+1$.*

Proof. Write π for the map $G \to G/N$. Then

$$\pi([...[[g_1, g_2], g_3], ..., g_m], g_{m+1}]) = [...[[\pi g_1, \pi g_2], \pi g_3], ..., \pi g_m], \pi g_{m+1}] = 1$$

all $g_1, ..., g_{m+1} \in G$. Hence $[...[[g_1, g_2], g_3], ..., g_m], g_{m+1}] \in N \subset Z(G)$, and so

$$[...[[g_1, g_2], g_3], ..., g_{m+1}], g_{m+2}] = 1 \text{ all } g_1, ..., g_{m+2} \in G.$$

□

Corollary 6.16. *A finite p-group is nilpotent.*

Proof. We use induction on the order of G. Then $G/Z(G)$ nilpotent $\implies G$ nilpotent. □

Theorem 6.17. *A finite group is nilpotent if and only if it is equal to a product of its Sylow subgroups.*

Proof. A product of nilpotent groups is (obviously) nilpotent, and so the necessity follows from the preceding corollary. Now assume that G is nilpotent. According to (5.10) it suffices to prove that all Sylow subgroups are normal. Let P be such a subgroup of G, and let $N = N_G(P)$. The first lemma below shows that $N_G(N) = N$, and the second then implies that $N = G$, i.e., that P is normal in G. □

Lemma 6.18. *Let P be a Sylow p-subgroup of a finite group G, and let $N = N_G(P)$. For any subgroup H with $N_G(P) \subset H \subset G$, we have $N_G(H) = H$.*

Proof. Let $g \in N_G(H)$, so that $gHg^{-1} = H$. Then $H \supset gPg^{-1} = P'$, which is a Sylow p-subgroup of H. By Sylow II, $hP'h^{-1} = P$ for some $h \in H$, and so $hgPg^{-1}h^{-1} \subset P$. Hence $hg \in N \subset H$, and $g \in H$. □

Lemma 6.19. *Let H be proper subgroup of a finite nilpotent group G; then $H \neq N_G(H)$.*

Proof. The statement is obviously true for commutative groups, and so we can assume G to be noncommutative. We use induction on the order of G. Because G is nilpotent, $Z(G) \neq 1$. Certainly the elements of $Z(G)$ normalize H, and so if $Z(G) \not\subseteq H$, we have $H \subsetneqq Z(G) \cdot H \subset N_G(H)$. Thus we may suppose $Z(G) \subset H$. Then the normalizer of H in G corresponds under (3.3) to the normalizer of $H/Z(G)$ in $G/Z(G)$, and we can apply the induction hypothesis. □

Remark 6.20. For a finite abelian group G we recover the fact that G is a product of its p-primary subgroups.

The next result is beloved of QR examiners.

Proposition 6.21 (Frattini's Argument). *Let H be a normal subgroup of a finite group G, and let P be a Sylow p-subgroup of H. Then $G = H \cdot N_G(P)$.*

Proof. Let $g \in G$. Then $gPg^{-1} \subset gHg^{-1} = H$, and both gPg^{-1} and P are Sylow p-subgroups of H. According to Sylow II, there is an $h \in H$ such that $gPg^{-1} = hPh^{-1}$, and it follows that $h^{-1}g \in N_G(P)$ and so $g \in H \cdot N_G(P)$. □

Theorem 6.22. *A finite group is nilpotent if and only if every maximal subgroup is normal.*

Proof. We saw in Lemma 6.19 that for any proper subgroup H of a nilpotent group G, $H \subsetneqq N_G(H)$. Hence, H maximal $\implies$ $N_G(H) = G$, i.e., H is normal in G.

Conversely, suppose every maximal subgroup of G is normal. We shall verify the criterion of Theorem 6.17. Thus, let P be a Sylow p-subgroup of G. Suppose P is not normal in G, and let H be a maximal subgroup of G containing $N_G(P)$. By hypothesis H is normal, and so Frattini's argument shows that $G = H \cdot N_G(P) = H$, which contradicts the definition of H. □

6.4. Groups with operators.

Recall that the set $\mathrm{Aut}(G)$ of automorphisms of a group G is again a group. If G is given together with a homomorphism $\varphi : A \to \mathrm{Aut}(G)$, then G is said to have A as a *group of operators*. The pair (G, φ) is also called an A-group.

Write ${}^{\alpha}x$ for $\varphi(\alpha)x$. Then

(a) ${}^{(\alpha\beta)}x = {}^{\alpha}({}^{\beta}x)$;
(b) ${}^{\alpha}(xy) = {}^{\alpha}x \cdot {}^{\alpha}y$;
(c) ${}^{1}x = x$.

Conversely, a map $(\alpha, x) \mapsto {}^{\alpha}x : A \times G \to G$ satisfying (a), (b), (c) arises from a homomorphism $A \to \mathrm{Aut}(G)$—conditions (a) and (c) show that $x \mapsto {}^{\alpha}x$ is inverse to $x \mapsto {}^{(\alpha^{-1})}x$, and so $x \mapsto {}^{\alpha}x$ is a bijection $G \to G$. Condition (b) then shows that it is an automorphism of G. Finally, (a) shows that the map $\varphi(\alpha) = (x \mapsto {}^{\alpha}x)$ is a homomorphism $A \to \mathrm{Aut}(G)$.

Let G be a group with operators A. A subgroup H of G is *admissible* or an *A-invariant subgroup* if $x \in H \implies {}^{\alpha}x \in H$, all $\alpha \in A$. An intersection of admissible groups is admissible. If H is admissible, so also are $N_G(H)$ and $C_G(H)$.

An *A-homomorphism* (or *admissible homomorphism*) of A-groups is a homomorphism $\varphi : G \to G'$ such that $\varphi({}^{\alpha}g) = {}^{\alpha}\varphi(g)$ for all $\alpha \in A$, $g \in G$.

Example 6.23. (a) A group G can be regarded as a group with $\{1\}$ as group of operators. In this case all subgroups and homomorphisms are admissible, and we see that the theory of groups with operators includes the theory of groups without operators.

(b) Consider G with G acting by conjugation, i.e., consider G together with $g \mapsto i_g : G \to \mathrm{Aut}(G)$. In this case, the admissible subgroups are the normal subgroups.

(c) Consider G with $A = \mathrm{Aut}(G)$ as group of operators. In this case, the admissible subgroups are the characteristic subgroups.

Almost everything we have proved in this course for groups also holds for groups with operators. In particular, the isomorphism theorems 3.1, 3.2, and 3.3 hold for groups with operators. In each case, the proof is the same as before except that admissibility must be checked.

Theorem 6.24. *(a) For any admissible homomorphism $\varphi : G \to G'$ of A-groups, $N = \mathrm{Ker}(\varphi)$ is an admissible normal subgroup of G, $\varphi(G)$ is an admissible subgroup of G', and φ factors in a natural way into the composite of an admissible surjection, an admissible isomorphism, and an admissible injection:*

$$G \twoheadrightarrow G/N \xrightarrow{\approx} \varphi(G) \hookrightarrow G'.$$

Theorem 6.25. *Let G be a group with operators A, and let H and N be admissible subgroups with N normal. Then $H \cap N$ is normal admissible subgroup of H, HN is an admissible subgroup of G, and $h(H \cap N) \mapsto hH$ is an admissible isomorphism $H/H \cap N \to HN/N$.*

Theorem 6.26. *Let $\varphi : G \to \bar{G}$ be a surjective admissible homomorphism of A-groups. Then under the one-to-one correspondence $H \leftrightarrow \bar{H}$ between the set of subgroups of G containing* $\mathrm{Ker}(\varphi)$ *and the set of subgroups of $\bar{G}$, admissible subgroups correspond to admissible subgroups.*

Let $\varphi : A \to \mathrm{Aut}(G)$ be a group with A operating. An *admissible normal series* is a sequence of admissible subgroups of G

$$G \supset G_1 \supset G_2 \supset \cdots \supset G_r$$

with each G_i normal in G_{i-1}. Define similarly an admissible composition series. The quotients of an admissible normal series are A-groups, and the quotients of an admissible composition series are simple A-groups, i.e., they have no normal admissible subgroups apart from the obvious two.

The Jordan-Hölder theorem continues to hold for A-groups. In this case the isomorphisms between the corresponding quotients of two composition series are admissible. The proof is the same as that of the original theorem, because it uses only the isomorphism theorems, which we have noted also hold for A-groups.

Example 6.27. (a) Consider G with G acting by conjugation. In this case an admissible normal series is a sequence of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_s = \{1\},$$

with each G_i normal in G. (This is what *should* be called a normal series.) The action of G on G_i by conjugation passes to the quotient, to give an action of G on G_i/G_{i+1}. The quotients of two admissible normal series are isomorphic as G-groups.

(b) Consider G with $A = \mathrm{Aut}(G)$ as operator group. In this case, an admisible normal series is a sequence

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_s = \{1\}$$

with each G_i a characteristic subgroup of G.

6.5. Krull-Schmidt theorem. A group G is *indecomposable* if $G \neq 1$ and G is not isomorphic to a product of two nontrivial subgroups, i.e., if

$$G \approx H \times H' \implies H = 1 \text{ or } H' = 1.$$

Example 6.28. (a) A simple group is indecomposable, but an indecomposable group need not be simple: it may have a normal subgroup. For example, S_3 is indecomposable but has C_3 as a normal subgroup.

(b) A finite abelian group is indecomposable if and only if it is cyclic of prime-power order.

Of course, this is obvious from the classification, but it is not difficult to prove it directly. Let G be cyclic of order p^n, and suppose that $G \approx H \times H'$. Then H and H' must be p-groups, and they can't both be killed by p^m, $m < n$. It follows that one must be cyclic of order p^n, and that the other is trivial. Conversely, suppose that G is abelian and indecomposable. Since every finite abelian group is (obviously) a product of p-groups with p running over the primes, we can assume G itself is a p-group. If g is an element of G of highest order, one shows that $<g>$ is a direct factor of G: $G \approx <g> \times H$ (see Rotman 4.5, 4.6, or Math 593).

(c) Every finite group can be written as a product of indecomposable groups (obviously).

Recall that when $G_1, G_2, \ldots, G_r$ are subgroups of G such that the map

$$(g_1, g_2, ..., g_r) \mapsto g_1 g_2 \cdots g_r : G_1 \times G_2 \times \cdots \times G_r \to G$$

is an isomorphism, then we write $G = G_1 \times G_2 \times \cdots \times G_r$.

Theorem 6.29 (Krull-Schmidt). *Let*

$$G = G_1 \times \cdots \times G_s \quad \text{and} \quad G = H_1 \times \cdots \times H_t$$

be two decompositions of G into products of indecomposable subgroups. Then $s = t$, and there is a re-indexing such that $G_i \approx H_i$. Moreover, given r, we can arrange the numbering so that

$$G = G_1 \times \cdots \times G_r \times H_{r+1} \times \cdots \times H_t.$$

Example 6.30. Let $G = \mathbb{F}_p \times \mathbb{F}_p$, and think of it as a two-dimensional vector space over $\mathbb{F}_p$. Let

$$G_1 = <(1,0)>, \quad G_2 = <(0,1)>; \quad H_1 = <(1,1)>, \quad H_2 = <(1,-1)> .$$

Then $G = G_1 \times G_2$, $G = H_1 \times H_2$, $G = G_1 \times H_2$.

Consider G with G acting by conjugation. Then an admissible subgroup is a normal subgroup, and a G-endomorphism $\alpha : G \to G$ is an endomorphism such that $\alpha(gxg^{-1}) = g\alpha(x)g^{-1}$ all g, $x \in G$. Such an endomorphism is called a *normal* endomorphism. A composite of normal endomorphisms is normal; the image of an admissible (i.e., normal) subgroup under a normal endomorphism is admissible (i.e., normal).

[[The rest of the notes are unreliable.]]

Let α be an endomorphism of a group G; then we have a descending sequence of subgroups

$$G \supset \alpha(G) \supset \alpha^2(G) \supset \cdots .$$

If G is finite it must become stationary. The endomorphism α is said to be *nilpotent* if $\alpha^k(G) = 1$ for some k. Note that if G is finite and $G = \alpha(G)$, then α is an automorphism.

Lemma 6.31 (Fitting). *Let G be a finite group and α a normal endomorphism. Choose k so that $\alpha^k(G) = \alpha^{k+1}(G) = \cdots$, and let $G_1 = \operatorname{Ker}(\alpha^k)$ and $G_2 = \alpha^k(G)$. Then $G = G_1 \times G_2$; moreover, $\alpha|G_1$ is nilpotent, and $\alpha|G_2$ is an automorphism.*

Proof. The final part of the statement is obvious from the above remarks. Therefore $g \in G_1 \cap G_2 \implies g = 1$ (else $\alpha^k(g)$ is never 1, and equals 1). Let $g \in G$. Then $\alpha^k(g) \in G_2 = \alpha^{k+1}G = \cdots$, and so $\alpha^k(g) = \alpha^{2k}(x)$ for some $x \in G$. Note that $\alpha^k(g \cdot \alpha^k(x^{-1})) = 1$, and so $g \cdot \alpha^k(x^{-1}) \in G_1$: we conclude $g = (g \cdot \alpha^k(g^{-1})) \cdot \alpha^k(g) \in G_1G_2$. Finally G_1 and G_2 are normal by the above remark, and now (3.6) implies that $G = G_1 \times G_2$. □

Lemma 6.32. *A normal endomorphism of an indecomposable finite group is either an automorphism or is nilpotent.*

Proof. In the preceding lemma, either $G = G_1$ or G_2. □

For endomorphisms α and β of a group G, define $\alpha + \beta$ by

$$(\alpha + \beta)(x) = \alpha(x)\beta(x).$$

Note: $\alpha + \beta$ need not be an endomorphism.

Lemma 6.33. *If α and β are normal nilpotent endomorphisms of a finite indecomposable group, and $\alpha + \beta$ is an endomorphism, then $\alpha + \beta$ is a normal nilpotent endomorphism.*

Proof. It is obvious that $\alpha + \beta$ is normal. If it is an automorphism, then there exists a γ such that $(\alpha + \beta) \circ \gamma = \mathrm{id}$. Set $\alpha' = \alpha\gamma$ and $\beta' = \beta\gamma$. Then $\alpha' + \beta' = \mathrm{id}$, i.e.,

$$\alpha'(x^{-1})\beta'(x^{-1}) = x^{-1} \implies \beta'(x)\alpha'(x) = x = \alpha'(x)\beta'(x) \implies \alpha'\beta' = \beta'\alpha'.$$

Hence $\alpha' + \beta' = \beta' + \alpha'$. Therefore the subring of $\operatorname{End}(G)$ generated by α' and β' is commutative. Because α and β are nilpotent, so also are α' and β'. Hence

$$(\alpha' + \beta')^m = \alpha'^m + \binom{m}{1}\alpha'^{m-1}\beta' + \cdots + \beta'^m$$

is zero for m sufficiently large. □

Proof. of Krull-Schmidt. Suppose $G = G_1 \times G_2 \times \cdots \times G_s$ and $G = H_1 \times H_2 \times \cdots \times H_t$. Write

$$\begin{tikzcd} G_i \arrow[r, shift left, "\iota_i"] & G_1 \times G_2 \times \cdots \times G_s, \arrow[l, shift left, "\pi_i"] & H_i \arrow[r, shift left, "\iota_i'"] & H_1 \times H_2 \times \cdots \times H_t. \arrow[l, shift left, "\pi_i'"] \end{tikzcd}$$

Consider $\pi_1\iota_1'\pi_1'\iota_1 + \pi_1\iota_2'\pi_2'\iota_1 + \cdots = \mathrm{id}_{G_1}$. Not all terms in the sum are nilpotent, and so, after possibly renumbering the groups, we may suppose that the first is an automorphism, say $\alpha = \pi_1\iota_1'\pi_1'\iota_1 = \gamma^{-1}$. Thus (omitting subscripts)

$$(G_1 \xrightarrow{\gamma} G_1 \xrightarrow{\iota} G \xrightarrow{\pi'} H_1 \xrightarrow{\iota'} G \xrightarrow{\pi} G_1) = \mathrm{id}_{G_1}.$$

Consider

$$(H_1 \xrightarrow{\iota'} G \xrightarrow{\pi} G_1 \xrightarrow{\gamma} G_1 \xrightarrow{\iota} G \xrightarrow{\pi'} H_1) = \theta.$$

Check $\theta \circ \theta = \theta$ (use above factorization of id_{G_1}), and so $\theta = \mathrm{id}$ or 0. The second is impossible, because θ occurs in $\mathrm{id}_{G_1} \circ \mathrm{id}_{G_1}$. Therefore, $\theta = \mathrm{id}_{H_1}$. Hence $\pi_1\iota_1'$ and $\pi_1'\iota_1$ are isomorphisms.

On the other hand, $\pi_1'(H_2 \times \cdots) = 1$, but $\pi_1'\iota_1 =?$ is injective on G_1. We conclude that $G_1 \cap (H_2 \times ... \times H_t) = 1$. Hence $G_1(H_2 \times \cdots) \approx G_1 \times (H_2 \times \cdots)$, and by counting, we see that $G = G_1 \times H_2 \times \cdots$.

Repeat the argument. □

Remark 6.34. (a) The Krull-Schmidt theorem holds also for an infinite group provided it satisfies both chain conditions on subgroups, i.e., ascending and descending sequences of subgroups of G become stationary. (See Rotman 6.33.)

(b) The Krull-Schmidt theorem also holds for groups with operators. For example, let $\mathrm{Aut}(G)$ operate on G; then the subgroups in the statement of the theorem will all be characteristic.

(c) When applied to a finite abelian group, the theorem shows that the groups C_{m_i} in a decomposition $G = C_{m_1} \times ... \times C_{m_r}$ are uniquely determined up to isomorphism (and ordering).