

1 Review of basic group theory

Almost all of the material in this chapter is in the syllabus for the level 3 course MAS305 Algebraic Structures II, and will therefore be treated mainly as revision. However, in practice not all of it may have been covered thoroughly in Algebraic Structures II, so please let me know how much detail you require me to give in the lectures as we go along. Also let me know if there are significant parts you have not seen before, that you need me to cover in more detail.

Groups, subgroups and cosets A *group* is a (finite) set G with an *identity* element 1 , a (binary) *multiplication* $x.y$ (or xy) and a (unary) *inverse* x^{-1} satisfying the *associative law* $(xy)z = x(yz)$, the *identity laws* $x1 = 1x = x$ and the *inverse laws* $xx^{-1} = x^{-1}x = 1$ for all $x, y, z \in G$ (and the *closure laws* $xy \in G$ and $x^{-1} \in G$ which we take for granted). It is *abelian* if $xy = yx$ for all $x, y \in G$, *non-abelian* otherwise. A *subgroup* is a subset H closed under multiplication and inverses. (It is sufficient to check $xy^{-1} \in H$ for all $x, y \in H$.) *Left cosets* of H in G are subsets $gH = \{gh \mid h \in H\}$ and *right cosets* are $Hg = \{hg \mid h \in H\}$. The left (or right) cosets all have the same size, and partition G , so that $|G| = |H||G : H|$ (*Lagrange's Theorem*), where $|G|$ is the *order* of G (i.e. the number of elements in G) and $|G : H|$ is the *index* of H in G , i.e. the number of left (or right) cosets. The *order* of an element $g \in G$ is the order n of the *cyclic group* $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$ it *generates*, and the *exponent* of G is the lowest common multiple of the orders of the elements, that is the smallest positive integer e such that $g^e = 1$ for all $g \in G$.

Homomorphisms and quotient groups A *homomorphism* is a map $\phi : G \rightarrow H$ which preserves the multiplication, $\phi(xy) = \phi(x)\phi(y)$ (from which it follows that $\phi(1) = 1$ and $\phi(x^{-1}) = \phi(x)^{-1}$). The *kernel* of ϕ is $\ker \phi = \{g \in G \mid \phi(g) = 1\}$, and is a subgroup which satisfies $g(\ker \phi) = (\ker \phi)g$, i.e. its left and right cosets are equal (such a subgroup N is called *normal*, written $N \trianglelefteq G$, or $N \triangleleft G$ if also $N \neq G$). An *isomorphism* is a bijective homomorphism, i.e. one satisfying $\ker \phi = \{1\}$ and $\phi(G) = H$: in this case we write $G \cong H$.

If N is a normal subgroup of G , the *quotient* group G/N has elements xN (for all $x \in G$) and group operations $(xN)(yN) = (xy)N$, and $(xN)^{-1} = x^{-1}N$. The *first isomorphism theorem* states that if $\phi : G \rightarrow H$ is a homomorphism then the image of ϕ , $\phi(G) \cong G/\ker\phi$ (and the isomorphism is given by $\phi(x) \mapsto x\ker\phi$).

The normal subgroups of G/N are in one-to-one correspondence with the normal subgroups K of G which contain N , and the *second isomorphism theorem* is $(G/N)/(K/N) \cong G/K$. If H is any subgroup of G , and N is any normal subgroup of G , then $HN = \{xy \mid x \in H, y \in N\}$ is a subgroup of G and $N \cap H$ is a normal subgroup of H , and the *third isomorphism theorem* is $HN/N \cong H/(N \cap H)$.

Simple groups and composition series A group S is *simple* if it has exactly two normal subgroups (1 and S). In particular, an abelian group is simple if and only if it has prime order. A series

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

for a group G is called a *composition series* if all the factors G_i/G_{i-1} are simple (and they are then called *composition factors*).

The *fourth isomorphism theorem* (or *Zassenhaus's butterfly lemma*) states that if $X \triangleleft Y \leq G$ and $A \triangleleft B \leq G$ then

$$\frac{(Y \cap B)X}{(Y \cap A)X} \cong \frac{(Y \cap B)}{(Y \cap A)(X \cap B)} \cong \frac{(Y \cap B)A}{(X \cap B)A}.$$

(We shall give two proofs of this in a moment.) Hence (see below) any two series for G have isomorphic *refinements*, and by induction on the length of a composition series, any two composition series for a finite group have the same composition factors, counted with multiplicities (the *Jordan–Hölder Theorem*). A *normal series* is one in which all terms G_i are normal in G , and if it has no proper refinements it is called a *chief series*, and its factors G_i/G_{i-1} *chief factors*.

Zassenhaus's butterfly lemma A proof of Zassenhaus's butterfly lemma goes as follows. Define the map $\phi : Y \cap B \rightarrow (Y \cap B)X/(Y \cap A)X$ by $\phi(y) = y(Y \cap A)X$. This is easily seen to be a group homomorphism (exercise: where does this use the fact that $X \triangleleft Y$? Where does it use the fact that $A \triangleleft B$?). Moreover, since $Y \cap A \subseteq Y \cap B$, it is easy to see that the image of ϕ is $(Y \cap B)X/(Y \cap A)X$. The tricky part of the proof is to identify the kernel of ϕ : we need to prove that $\ker\phi = (Y \cap A)(X \cap B)$. On the one hand, if $y \in Y \cap A$ then $\phi(y)$ is the identity coset $(Y \cap A)X$. Similarly, if $y \in X \cap B$ then $\phi(y) = y(Y \cap A)X \subseteq X(Y \cap A)X \subseteq (Y \cap A)X$ since $X \triangleleft Y$. Therefore $(Y \cap A)(X \cap B) \subseteq \ker\phi$. Conversely, if $y \in \ker\phi$ then $y \in (Y \cap A)X$, so we can write $y = ax$ with $a \in Y \cap A$ and $x \in X$. But now $y \in B$ and $a \in B$ so $x \in B$ and therefore $y \in (Y \cap A)(X \cap B)$, showing that $\ker\phi \subseteq (Y \cap A)(X \cap B)$. So we have $\ker\phi = (Y \cap A)(X \cap B)$ and the result follows from the first isomorphism theorem.

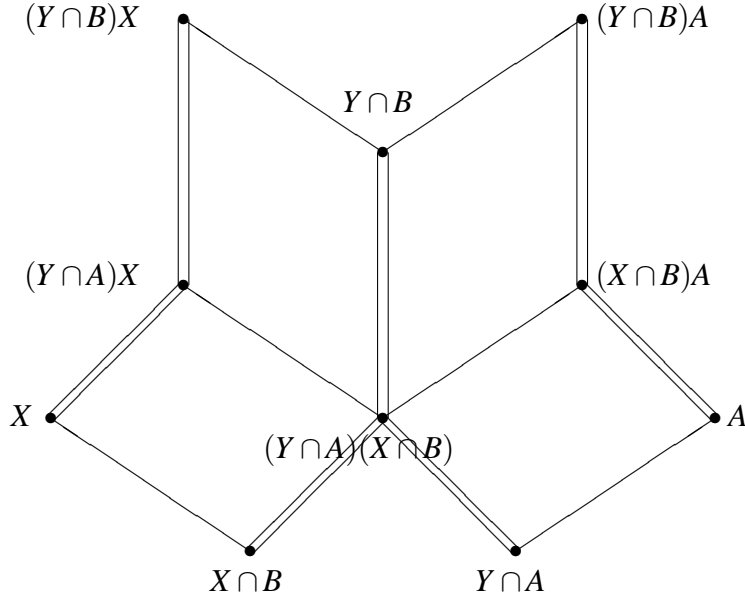


Figure 1: Zassenhaus's butterfly

In Figure 1, single lines represent subgroups, and double lines represent normal subgroups. For example, X is normal in $(Y \cap A)X$, since X is normal in Y , but $X \cap B$ is not necessarily normal in X . More accurately, the double lines represent *quotient groups*, and any two parallel double lines represent isomorphic quotient groups. The isomorphisms of the vertical lines are given by Zassenhaus's butterfly lemma. The bottom two parallelograms consist of two instances of isomorphisms of the form $PQ/Q \cong P/(P \cap Q)$. Indeed, so do the top two parallelograms, although this is not so easy to see.

To prove the last statement (and hence get an alternative proof of Zassenhaus's lemma using the third isomorphism theorem) use the so-called *Dedekind modular law*: if P , Q , and R are subgroups of a group G , and $R \subseteq P$, then $P \cap (QR) = (P \cap Q)R$. Proof: if $x \in (P \cap Q)R$ then $x = yz$ with $y \in P \cap Q \subseteq P$ and $z \in R \subseteq P$, so $x \in P$; clearly $x \in QR$, so $x \in P \cap (QR)$. Conversely, if $x \in P \cap QR$ then $x = qr$ with $q \in Q$ and $r \in R \subseteq P$, and therefore $q = xr^{-1} \in P$, so $x \in (P \cap Q)R$.

Now to deduce Zassenhaus's lemma, observe that by Dedekind's law, $(Y \cap B) \cap A(X \cap B) = (Y \cap B \cap A)(X \cap B) = (Y \cap A)(X \cap B)$. Then the result follows from the third isomorphism theorem.

The Jordan–Hölder Theorem We use Zassenhaus's lemma to prove the Jordan–Hölder theorem. If

$$\begin{aligned} 1 = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_{n-1} \triangleleft G_n = G \\ 1 = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_{m-1} \triangleleft H_m = G \end{aligned} \quad (2)$$

are two composition series of G , then we use the second series to refine the first: in the gap between G_i and G_{i+1} we put the series

$$G_i = (G_{i+1} \cap H_0)G_i \trianglelefteq (G_{i+1} \cap H_1)G_i \trianglelefteq (G_{i+1} \cap H_2)G_i \trianglelefteq \cdots \trianglelefteq (G_{i+1} \cap H_{m-1})G_i \trianglelefteq (G_{i+1} \cap H_m)G_i = G_{i+1} \quad (3)$$

Similarly, we use the first series to refine the second: in the gap between H_j and H_{j+1} we put the series

$$H_j = (H_{j+1} \cap G_0)H_j \trianglelefteq (H_{j+1} \cap G_1)H_j \trianglelefteq (H_{j+1} \cap G_2)H_j \trianglelefteq \cdots \trianglelefteq (H_{j+1} \cap G_{n-1})H_j \trianglelefteq (H_{j+1} \cap G_n)H_j = H_{j+1} \quad (4)$$

Then Zassenhaus's lemma says the quotients in the refinement of the first series are equal (in some order) to the quotients in the refinement of the second series. Most of these quotients will be the trivial group: deleting repetitions gives back the two composition series.

Soluble groups A group is *soluble* if it has a composition series with abelian (hence cyclic of prime order) composition factors. A *commutator* is an element $x^{-1}y^{-1}xy$, denoted $[x, y]$, and the subgroup generated by all commutators $[x, y]$ of elements $x, y \in G$ is the *commutator subgroup* (or *derived subgroup*), written $[G, G]$ or G' . Writing $G^{(0)} = G$ and $G^{(n)} = (G^{(n-1)})'$, it follows that G is soluble if and only if $G^{(n)} = 1$ for some n . Also G/N is abelian if and only if N contains G' , so G/G' is the *largest abelian quotient* of G .

Group actions and conjugacy classes The *right regular representation* of a group G is the identification of each element $g \in G$ with the permutation $x \mapsto xg$ of the elements of G . This shows that every finite group is isomorphic to a group of permutations (*Cayley's theorem*). If G is a group of permutations on a set Ω , and $a \in \Omega$, the *stabilizer* of a is the subgroup H of all permutations in G which map a to itself. Then Lagrange's theorem can be re-written as the *orbit-stabilizer theorem*, that $|G|/|H|$ equals the number of images of a under G (i.e. the *length* of the *orbit* of a).

More generally, we say a group G *acts on* a set Ω if there is a homomorphism ϕ from G to a subgroup of $\text{Sym}\Omega$. If $\ker\phi = 1$ we say the action is *faithful*; in this case G is isomorphic to the image of ϕ , and we might as well say $G = \text{im}\phi$.

Now let G act on itself by conjugation, $g : x \mapsto g^{-1}xg$, so that the orbits are the *conjugacy classes* $[x] = \{g^{-1}xg \mid g \in G\}$, and the stabilizer of x is the *centralizer* of x , $C_G(x) = \{g \in G \mid g^{-1}xg = x\}$. In particular, the conjugacy classes partition G , and their sizes divide the order of G . An element x is in a conjugacy class of size 1 if and only if x *commutes* with every element of G , i.e. $x \in Z(G) = \{y \in G \mid g^{-1}yg = y \text{ for all } g \in G\}$, the *centre* of G , which is a normal subgroup of G . Indeed, the centre of G is exactly the kernel of the given action.

p -groups and nilpotent groups A finite group is called a p -group if its order is a power of the prime p (and so by Lagrange's Theorem all its elements have order some power of p). Every conjugacy class in G has p^a elements for some a , and $\{1\}$ is a conjugacy class, so there are at least p conjugacy classes of size 1, and $Z(G)$ has order at least p . Define $Z_1(G) = Z(G)$ and $Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$, so that if G is a p -group then $Z_n(G) = G$ for some n . A group with this property is called *nilpotent* (of class at most n), and the series

$$1 = Z_0(G) \triangleleft Z_1(G) \triangleleft Z_2(G) \triangleleft \cdots$$

is called the *upper central series*.

The *direct product* $G_1 \times \cdots \times G_k$ of groups G_1, \dots, G_k is defined on the set $\{(g_1, \dots, g_k) \mid g_i \in G_i\}$ by the group operations $(g_1, \dots, g_k)(h_1, \dots, h_k) = (g_1h_1, \dots, g_kh_k)$ and $(g_1, \dots, g_k)^{-1} = (g_1^{-1}, \dots, g_k^{-1})$. A finite group is nilpotent if and only if it is a direct product of p -groups.

Sylow's theorems If G is a finite group of order $p^k n$, where p is prime and n is not divisible by p , then the *Sylow theorems* state that

- (a) G has subgroups of order p^k , called *Sylow p -subgroups*;
- (b) these Sylow p -subgroups are all conjugate; and
- (c) the number s_p of Sylow p -subgroups satisfies $s_p \equiv 1 \pmod{p}$. (Note also that, by the orbit-stabilizer theorem, s_p is a divisor of n).

To prove the first statement, let G act by right multiplication on all subsets of G of size p^k : since the number of these subsets is not divisible by p , there is a stabilizer of order divisible by p^k , and therefore equal to p^k . To prove the second statement, and also to prove that any p -subgroup is contained in a Sylow p -subgroup, let any p -subgroup Q act on the right cosets Pg of any Sylow p -subgroup P by right multiplication: since the number of cosets is not divisible by p , there is an orbit $\{Pg\}$ of length 1, so $PgQ = Pg$ and gQg^{-1} lies inside P . To prove the third statement, let a Sylow p -subgroup P act by conjugation on the set of all the other Sylow p -subgroups: the orbits have length divisible by p , for otherwise P and Q are distinct Sylow p -subgroups of $N_G(Q)$, which is a contradiction.

An important corollary of Sylow's theorems is the *Fratini argument*: if $N \triangleleft G$ and P is a Sylow p -subgroup of N , then $G = N_G(P)N$.

Automorphism groups An *automorphism* of a group G is just an isomorphism of G with itself. The set of all automorphisms of G is easily seen to form a group under composition, and is denoted $\text{Aut}(G)$. The *inner* automorphisms are the automorphisms ϕ_g for $g \in G$, defined by $\phi_g : x \mapsto g^{-1}xg$. These form a subgroup $\text{Inn}(G)$ of $\text{Aut}(G)$. Indeed, if $\alpha \in \text{Aut}(G)$, then it is easy to check that $\phi_g^\alpha = \phi_{g^\alpha}$ (where $\phi_g^\alpha = \alpha^{-1}\phi_g\alpha$, read

from left to right for conformity with our notation for permutations), so that $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$.

Now it is easy to check that $\phi_{gh} = \phi_g \phi_h$, and that $\phi_g = \phi_h$ if and only if $gh^{-1} \in Z(G)$, so the map ϕ defined by $\phi : g \mapsto \phi_g$ is a homomorphism from G onto $\text{Inn}(G)$ with kernel $Z(G)$. Therefore $\text{Inn}(G) \cong G/Z(G)$ and, in particular, if $Z(G) = 1$ then $G \cong \text{Inn}(G)$. In this case, we can therefore identify G with $\text{Inn}(G)$, and thus embed G as a normal subgroup of $\text{Aut}(G)$.

We define $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$, called the *outer automorphism group* of G . Note that, despite its name, its elements are not automorphisms! It is a quotient group, not a subgroup, of $\text{Aut}(G)$.