MT5824 Topics in Groups

MQ

September 25, 2020

Contents

Introduction

The purpose of this course is to take the study of groups further beyond the contents of the previous course. Accordingly, we note:

Prerequisite: MT4003

The goal of the course will be to introduce a variety of topics in more advanced group theory. We shall particularly be interested in topics that have some relation to the research of the group theorists in St Andrews.

The topics considered will be as follows:

Revision: Review of the basic concepts of subgroup, normal subgroup, quotient group and homomorphism. (Some new results will be proved which will used later in the course.)

Group Actions: We will explain how a group can induced permutations of a set and deduce structural properties about subgroups and homomorphisms.

Sylow's Theorem: We review Sylow's Theorem from the group action viewpoint and illustrate some applications.

Composition series: We consider how a group can be decomposed into essentially uniquely determined simple groups. This illustrates one example of a "series" for a group.

Building groups: We discuss how groups may be constructed and in particular some ways in which the above decomposition may be reversed. We shall review the direct product construction but also generalise it.

Soluble groups: We meet a particular class of groups that has a fairly restricted structure. We shall prove Hall's Theorem (a generalisation of Sylow's Theorem for soluble groups).

Nilpotent groups: We finish by discussing an even more restricted class of groups, of which the typical example is the p-group.

Themes: There will be two main themes which we shall attempt to exploit during the course.

(i) *Group Actions:* essentially this boils down to a group inducing certain permutations of a set and using this to obtain information about the original group.

(ii) *Series:* If a group G has a collection of subgroups

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

where G_{i+1} is a normal subgroup of G_i for all i, then information about the quotient groups G_i/G_{i+1} $(0 \leqslant i \leqslant n-1)$ yields information about G.

Recommended Texts: The following textbooks are appropriate and possibly useful for consultation. Only the first two are cheap enough to consider buying!

- John S. Rose, *A Course on Group Theory* (Dover Publications, New York, 1994), £6.50, QA171.R7.
- B. A. F. Wehrfritz, *Finite Groups: A Second Course on Group Theory* (World Scientific, Singapore, 1999), £18, not in library.
- Derek J. S. Robinson, *A Course in the Theory of Groups (Second Edition)*, Graduate Texts in Mathematics **80** (Springer–Verlag, New York, 1996), £52.50, QA171.R73.
- Joseph J. Rotman, *The theory of groups: an introduction* (Allyn & Bacon, 1965). QA171.R7.
- M. I. Kargapolov & Ju. I. Merzljakov, *Fundamentals of the Theory of Groups*, Graduate Texts in Mathematics **62** (Springer–Verlag, New York, 1979). QA171.K28M4

Section 1

Revision and Re-Activation

In this first section I shall principally recall definitions and results from earlier lecture courses. Often I will omit the proof of results that have been previously met during the lectures (though these notes will contain them). I shall also establish the notation to be used throughout the course. In a number of places I will be deviating slightly from that met in some of the earlier courses, but I hope that I am being more consistent with typical usage in the mathematical community when I do so.

Definition 1.1 A *group* G is a set with a binary operation (usually written multiplicatively)

$$\begin{aligned} G \times G &\to G \\ (x, y) &\mapsto xy \end{aligned}$$

such that

(i) the binary operation is *associative*:

$$x(yz) = (xy)z \qquad \text{for all } x, y, z \in G;$$

(ii) there is an *identity element* 1 in G:

$$x1 = 1x = x \qquad \text{for all } x \in G;$$

(iii) each element x in G possesses an *inverse* x^{-1}:

$$xx^{-1} = x^{-1}x = 1.$$

Comments:

(i) I have made no reference to 'closure' explicity as an axiom. The reason for this is that this condition is actually built into the definition of a binary operation. A binary operation takes two elements of our group and creates a third element *in the group*, and so we have closure automatically.

(ii) Associativity ensures that we can safely omit brackets from a product $x_1 x_2 \dots x_n$ of n elements x_1, x_2, …, x_n of a group. Thus, for example, the following products are all equal:

$$x_1(x_2(x_3x_4)), \qquad (x_1(x_2x_3))x_4, \qquad ((x_1x_2)x_3)x_4, \qquad \text{etc.}$$

(iii) We can define powers x^n where $x \in G$ and $n \in \mathbb{Z}$. Standard power laws hold although we need to remember that in general group elements do not commute (so, for example, we cannot easily expand $(xy)^n$) although we can expand the following inverse:

$$(xy)^{-1} = y^{-1}x^{-1}.$$

[Proof [Omitted in lectures]:

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

so multiplying on the right by the inverse of xy yields $y^{-1}x^{-1} = (xy)^{-1}$.]

For completeness, let us record the term used for groups where all the elements present do commute:

Definition 1.2 A group G is called *abelian* if all its elements *commute*; that is, if

$$xy = yx \qquad \text{for all } x, y \in G.$$

Subgroups

Although one is initially tempted to attack groups by examining their elements, this turns out not to be terribly fruitful. Even an only moderately sized group is unyielding to consideration of its multiplication table. Instead one needs to find some sort of "structure" to study and this is provided by subgroups and homomorphisms (and, particularly related to the latter, quotient groups).

A subgroup of a group is a subset which is itself a group under the multiplication inherited from the larger group. Thus:

Definition 1.3 A subset H of a group G is a *subgroup* of G if

(i) H is non-empty,

(ii) $xy \in H$ and $x^{-1} \in H$ for all $x, y \in H$.

We write $H \leqslant G$ to indicate that H is a subgroup of G. If G is a group, the set containing the identity element (which I shall denote by $\mathbf{1}$) and the whole group are always subgroups. We shall usually be interested in finding other subgroups of a group.

We mention in passing that the above conditions for a subset to be a subgroup are not the only ones used, but they are sufficient for our needs (and easily memorable).

The identity element of G lies in every subgroup, so it is easy to see that the conditions of Definition **??** are inherited by intersections. Therefore:

Lemma 1.4 *If $\{\, H_i \mid i \in I \,\}$ is a collection of subgroups of a group G, then $\bigcap_{i \in I} H_i$ is also a subgroup of G.*

Proof: [Omitted in lectures] We have $1 \in H_i$ for all i, so $\bigcap_{i \in I} H_i \neq \varnothing$. Now let $x, y \in \bigcap_{i \in I} H_i$. Then for each i, $x, y \in H_i$, so $xy \in H_i$ and $x^{-1} \in H_i$ since $H_i \leqslant G$. We deduce that $xy \in \bigcap_{i \in I} H_i$ and $x^{-1} \in \bigcap_{i \in I} H_i$. Thus the intersection is a subgroup. □

In general, the union of a family of subgroups of a group is not itself a subgroup. This is not a disaster, however, as the following construction provides a way around this.

Definition 1.5 Let G be a group and X be a subset of G. The *subgroup of G generated by X* is denoted by $\langle X \rangle$ and is defined to be the intersection of all subgroups of G which contain X.

Lemma **??** ensures that $\langle X \rangle$ is a subgroup of G. It is the smallest subgroup of G containing X (in the sense that it is contained in all other such subgroups; that is, if H is any subgroup of G containing X then $\langle X \rangle \leqslant H$).

Lemma 1.6 *Let G be a group and X be a subset of G. Then*

$$\langle X \rangle = \{\, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} \mid n \geqslant 0,\ x_i \in X,\ \varepsilon_i = \pm 1 \text{ for all } i \,\}.$$

Thus $\langle X \rangle$ consists of all products of elements of X and their inverses.

Proof: [Omitted in lectures] Let S denote the set on the right-hand side. Since $\langle X \rangle$ is a subgroup (by Lemma **??**) and by definition it contains X, we deduce that $\langle X \rangle$ must contain all products of elements of X and their inverses. Thus $S \subseteq \langle X \rangle$.

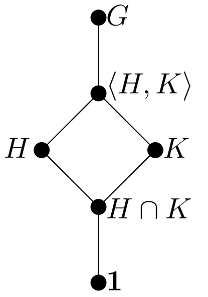
On the other hand, S is non-empty (for example, it contains the empty product (where $n = 0$) which by convention is taken to be the identity element 1), it contains all elements of X (the case $n = 1$ and $\varepsilon_1 = 1$), is clearly closed under products and

$$(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n})^{-1} = x_n^{-\varepsilon_n} x_{n-1}^{-\varepsilon_{n-1}} \dots x_1^{-\varepsilon_1} \in S.$$

Hence S is a subgroup of G. The fact that $\langle X \rangle$ is the smallest subgroup containing X now gives $\langle X \rangle \leqslant S$ and we deduce the equality claimed in the lemma. □

Now if H and K are subgroups of G, we have $\langle H, K \rangle$ available as the smallest subgroup of G that contains both H and K. We usually use this instead of the union.

We will wish to manipulate the subgroups of a group and understand how they relate to each other. Useful in such a situation are diagrams where we represent subgroups by nodes and use an upward line to denote inclusion. For example, the following illustrates the phenomena just discussed:



(For subgroups H and K of G, we have $H \cap K$ as the largest subgroup contained in H and K, and $\langle H, K \rangle$ as the smallest subgroup containing H and K.)

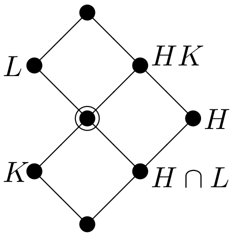
Before discussing more familiar concepts from previous courses, we prove a result that is extremely useful when manipulating subgroups.

Lemma 1.7 (Dedekind's Modular Law) *Let G be a group and H, K and L be subgroups of G with $K \leqslant L$. Then*

$$HK \cap L = (H \cap L)K.$$

(Here we define $HK = \{ hk \mid h \in H,\ k \in K \}$. A similar formula defines the set product $(H \cap L)K$.)

As an *aide memoire*, the following diagram can be used to remember the formula:



The circled node represents both $HK \cap L$ and $(H \cap L)K$. (The diagram is slightly misleading in the context of the previous discussion: HK (and the other products appearing) need not be a subgroup, but the diagram is at least useful to remember the result.)

PROOF: $H \cap L \leqslant H$, so immediately we have $(H \cap L)K \subseteq HK$. Also $H \cap L$ and K are contained in L, so $(H \cap L)K \subseteq L$ (since L is closed under products). Thus

$$(H \cap L)K \subseteq HK \cap L.$$

Now let $x \in HK \cap L$. Then $x = hk$ where $h \in H$ and $k \in K$. Now $h = xk^{-1} \in L$ since $x \in L$ and $k \in K \leqslant L$. Thus $h \in H \cap L$ and so $x = hk \in (H \cap L)K$. □

Cosets

Subgroups enforce a rigid structure on a group: specifically a group is the disjoint union of the cosets of any particular subgroup. Accordingly we need the following definition.

Definition 1.8 Let G be a group, H be a subgroup of G and x be an element of G. The (*right*) *coset* of H with *representative* x is the subset

$$Hx = \{\, hx \mid h \in H \,\}$$

of G.

We can equally well define what is meant by a left coset, but we shall work almost exclusively with right cosets. For the latter reason we shall simply use the term 'coset' and always mean 'right coset'.

Theorem 1.9 *Let G be a group and H be a subgroup of G.*

(i) *If $x, y \in G$, then $Hx = Hy$ if and only if $xy^{-1} \in H$.*

(ii) *Any two cosets of H are either equal or are disjoint: if $x, y \in G$, then either $Hx = Hy$ or $Hx \cap Hy = \varnothing$.*

(iii) *G is the disjoint union of the cosets of H.*

(iv) *If $x \in G$, the map $h \mapsto hx$ is a bijection from H to the coset Hx.*

PROOF: [OMITTED IN LECTURES] (i) Suppose $Hx = Hy$. Then $x = 1x \in Hx = Hy$, so $x = hy$ for some $h \in H$. Thus $xy^{-1} = h \in H$.

Conversely if $xy^{-1} \in H$, then $hx = h(xy^{-1})y \in Hy$ for all $h \in H$, so $Hx \subseteq Hy$. Also $hy = hyx^{-1}x = h(xy^{-1})^{-1}x \in Hx$ for all $h \in H$, so $Hy \subseteq Hx$. Thus $Hx = Hy$ under this assumption.

(ii) Suppose that $Hx \cap Hy \neq \varnothing$. Then there exists $z \in Hx \cap Hy$, say $z = hx = ky$ for some $h, k \in H$. Then $xy^{-1} = h^{-1}k \in H$ and we deduce $Hx = Hy$ by (i).

(iii) If $x \in G$, then $x = 1x \in Hx$. Hence the union of all the (right) cosets of H is the whole of G. Part (ii) ensures this is a disjoint union.

(iv) By definition of the coset Hx, the map $h \mapsto hx$ is a surjective map from H to Hx. Suppose $hx = kx$ for some $h, k \in H$. Then multiplying on the right by x^{-1} yields $h = k$. Thus this map is also injective, so it is a bijection, as claimed. □

Write $|G : H|$ for the number of cosets of H in G and call this the *index* of H in G. The previous result tells us that our group G is the disjoint union of $|G : H|$ cosets of H and each of these contain $|H|$ elements. Hence:

Theorem 1.10 (Lagrange's Theorem) *Let G be a group and H be a subgroup of G. Then*

$$|G| = |G : H| \cdot |H|.$$

In particular, if H is a subgroup of a finite group G, then the order of H divides the order of G. □

At this point we insert two results about the index of subgroups. The first is frequently used while the second will be needed (much) later in the course.

Lemma 1.11 *Let H and K be subgroups of a group G with $K \leqslant H \leqslant G$. Then*

$$|G : K| = |G : H| \cdot |H : K|.$$

I shall omit the proof (both in the lectures and these notes). In full generality, it appears on Problem Sheet I, while for finite groups it is easily deduced from Lagrange's Theorem.

Lemma 1.12 *Let G be a group and H and K be subgroups of G. Then*

$$|G : H \cap K| \leqslant |G : H| \cdot |G : K|.$$

Furthermore, if $|G : H|$ and $|G : K|$ are coprime integers, then

$$|G : H \cap K| = |G : H| \cdot |G : K|.$$

PROOF: Define a map from the set of cosets of $H \cap K$ to the Cartesian product of the sets of cosets of H and of K by

$$\phi \colon (H \cap K)x \mapsto (Hx, Kx).$$

Now

$$\begin{aligned}(H \cap K)x = (H \cap K)y \quad &\text{if and only if} \quad xy^{-1} \in H \cap K \\ &\text{if and only if} \quad xy^{-1} \in H \text{ and } xy^{-1} \in K \\ &\text{if and only if} \quad Hx = Hy \text{ and } Kx = Ky.\end{aligned}$$

So ϕ is well-defined and injective. Therefore

$$|G : H \cap K| \leqslant |G : H| \cdot |G : K|. \tag{1.1}$$

Now suppose that $|G : H|$ and $|G : K|$ are coprime integers. First note that Equation (**??**) tells us that $|G : H \cap K|$ is an integer. We need to establish the reverse inequality. Now $H \cap K \leqslant H \leqslant G$, so

$$|G : H \cap K| = |G : H| \cdot |H : H \cap K|$$

by Lemma **??**. It follows that $|G : H \cap K|$ is divisible by $|G : H|$. It is similarly divisible by $|G : K|$. As these integers are coprime, we deduce

$$|G : H| \cdot |G : K| \text{ divides } |G : H \cap K|.$$

This establishes the required reverse inequality and completes the proof when taken together with Equation (**??**). □

Orders of elements and Cyclic groups

Definition 1.13 If G is a group and x is an element of G, we define the *order* of x to be the smallest positive integer n such that $x^n = 1$ (if such exists) and otherwise say that x has *infinite order*.

We write $o(x)$ for the order of the element x.

If $x^i = x^j$ for $i < j$, then $x^{j-i} = 1$ and x has finite order and $o(x) \leqslant j - i$. In particular, the powers of x are always distinct if x has infinite order.

If x has finite order n and $k \in \mathbb{Z}$, write $k = nq + r$ where $0 \leqslant r < n$. Then

$$x^k = x^{nq+r} = (x^n)^q x^r = x^r \tag{1.2}$$

(since $x^n = 1$). Furthermore $1, x, x^2, \ldots, x^{n-1}$ are distinct (by the first line of the previous paragraph). Hence:

Proposition 1.14 (i) *If $x \in G$ has infinite order, then the powers x^i (for $i \in \mathbb{Z}$) are distinct.*

(ii) *If $x \in G$ has order n, then x has precisely n distinct powers, namely $1, x, x^2, \ldots, x^{n-1}$.* □

Corollary 1.15 *Let G be a group and $x \in G$. Then*

$$o(x) = |\langle x \rangle|.$$

If G is a finite group, then $o(x)$ divides $|G|$. □

Equation (**??**) yields a further observation, namely:

$$x^k = 1 \qquad \text{if and only if} \qquad o(x) \mid k.$$

In the case that a single element generates the whole group, we give a special name:

Definition 1.16 A group G is called *cyclic* (with *generator* x) if $G = \langle x \rangle$.

Using ideas as just described, it is reasonably easy to establish the following (and also a corresponding result for infinite cyclic groups):

Theorem 1.17 *Let G be a finite cyclic group of order n. Then G has precisely one subgroup of order d for every divisor d of n.*

The proof of this theorem is omitted. It, and more, can be found on Problem Sheet I.

Normal subgroups and quotient groups

Definition 1.18 A subgroup N of a group G is called a *normal subgroup* of G if $g^{-1}xg \in N$ for all $x \in N$ and all $g \in G$. We write $N \trianglelefteqslant G$ to indicate that N is a normal subgroup of G.

The element $g^{-1}xg$ is called the *conjugate* of x by g and is often denoted by x^g. We shall discuss this in greater detail in Section **??**.

If $N \trianglelefteqslant G$, then we write G/N for the set of cosets of N in G:

$$G/N = \{ Nx \mid x \in G \}.$$

Theorem 1.19 *Let G be a group and N be a normal subgroup of G. Then*

$$G/N = \{ Nx \mid x \in G \},$$

the set of cosets of N in G, is a group when we define the multiplication by

$$Nx \cdot Ny = Nxy$$

for $x, y \in G$.

PROOF: [OMITTED IN LECTURES] The part of this proof requiring the most work is to show that this product is actually well-defined. Suppose that $Nx = Nx'$ and $Ny = Ny'$ for some elements $x, x', y, y' \in G$. Then $x = ax'$ and $y = by'$ for some $a, b \in N$. Then

$$xy = (ax')(by') = ax'b(x')^{-1}x'y' = ab^{(x')^{-1}}x'y'.$$

Since $N \trianglelefteq G$, we have $b^{(x')^{-1}} \in N$. Hence $(xy)(x'y')^{-1} = ab^{(x')^{-1}} \in N$ and we deduce $Nxy = Nx'y'$. This shows that the above multiplication of cosets is indeed well-defined.

It remains to show that the set of cosets forms a group under this multiplication. If $x, y, z \in G$, then

$$(Nx \cdot Ny) \cdot Nz = Nxy \cdot Nz = N(xy)z = Nx(yz) = Nx \cdot Nyz = Nx \cdot (Ny \cdot Nz).$$

Thus the multiplication is associative. We calculate

$$Nx \cdot N1 = Nx1 = Nx = N1x = N1 \cdot Nx$$

for all cosets Nx, so $N1$ is the identity element in G/N, while

$$Nx \cdot Nx^{-1} = Nxx^{-1} = N1 = Nx^{-1}x = Nx^{-1} \cdot Nx,$$

so Nx^{-1} is the inverse of Nx in G/N.

Thus G/N is a group. □

Definition 1.20 If G is a group and N is a normal subgroup of G, we call G/N (with the above multiplication) the *quotient group* of G by N.

We shall discuss quotient groups later in this section. They are best discussed, however, in the context of homomorphisms, so we shall move onto these in a moment. I shall just mention some results (one part of which I shall prove, the rest appear on Problem Sheet I) which will be needed later.

Lemma 1.21 *Let G be a group and let H and K be subgroups of G. Define $HK = \{\, hk \mid h \in H,\ k \in K \,\}$. Then*

(i) *HK is a subgroup of G if and only if $HK = KH$;*

(ii) *if K is a normal subgroup of G then HK is a subgroup of G (and consequently $HK = KH$);*

(iii) *if H and K are normal subgroups of G, then $H \cap K$ and HK are normal subgroups of G;*

(iv) *$|HK| \cdot |H \cap K| = |H| \cdot |K|$.*