Part III Infinite Groups - Notes for preparation

Henry Bradford

August 27, 2021

These notes are intended for the use of students starting the course "Part III Infinite Groups". They are intended to cover concepts which are present in most, but not all undergraduate curricula in Group Theory, and a few basic facts about metric spaces which we shall use during the course. I anticipate that the majority of students will be familiar with a large part of this material, but only a minority will be comfortable with all of it already. Students should check that they understand everything in these notes, and can reproduce the proofs that I have omitted, as these concepts will be used frequently and without further comment throughout the course.

Throughout, G is a group.

Definition 1. *Let $H \leq G$. A* (left) coset *of H in G is a subset of G of the form:*

$$gH = \{gh : h \in H\}$$

for some $g \in G$. The set of all cosets is denoted G/H; its cardinality, denoted $|G : H|$, is the index *of H in G.*

Proposition 2. *For $g_1, g_2 \in G$, either $g_1 H = g_2 H$ or $g_1 H \cap g_2 H = \emptyset$.*

Definition 3. *A* transversal *to H in G is a subset $T \subseteq G$ such that for all $C \in G/H$, $|C \cap T| = 1$.*

Lemma 4. *For T any transversal to H in G,*

$$G = \coprod_{t \in T} tH$$

and $|T| = |G : H|$.

Lemma 5. *Let $H, K \leq G$. Then:*

(i) $|H : H \cap K| \leq |G : K|$;

(ii) *If* $K \leq H$ *then* $|G : K| = |G : H||H : K|$.

Notation 6. *We write* $H \leq_f G$ *(respectively* $H \lhd_f G$*) if* $H \leq G$ *(resp.* $H \lhd G$*) and* $|G : H| < \infty$.

Proposition 7. *Let* $H \leq_f G$. *Then there exists* $N \lhd_f G$ *with* $N \leq H$.

Proof. We give two proofs.

Proof # 1: Let T be a transversal to H in G. Let:

$$N = \bigcap_{t \in T} tHt^{-1}.$$

The index of N in G is finite by Lemma 5 (i); the other conditions are clear.

Proof # 2: G acts on G/H by left-multiplication: the action $G \times G/H \to G/H$ is given by $g(tH) = (gt)H$. The stabilizer of the point $H \in G/H$ under this action is precisely H. There is an induced homomorphism $\phi : G \to \mathrm{Sym}(G/H)$. Then $N = \ker(\phi)$ satisfies the required conditions. □

Exercise 8. *Give an upper bound for* $|G : N|$ *in terms of* $|G : H|$ *(which of the two above proofs yields the better bound?).*

Definition 9. *Let* $S \subseteq G$. *The* subgroup of G generated by S *is:*

$$\langle S \rangle = \left\{ s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n} : n \in \mathbb{N}, s_i \in S, \epsilon_i \in \{\pm 1\} \right\}$$

If $\langle S \rangle = G$ *we say* S *is a* generating set *for* G. G *is* finitely generated *if it has a finite generating set.*

Proposition 10. *The set* $\langle S \rangle$ *is indeed a subgroup of* G. *It is the smallest subgroup of* G *containing* S, *in the sense that: (i)* $S \subseteq \langle S \rangle$, *and (ii) whenever* $S \subseteq H \leq G$, *we have* $\langle S \rangle \leq H$.

Proposition 11. *Suppose* G *is a finitely generated group, and let* $S \subseteq G$ *be a (not necessarily finite) generating set. Then there exists* $S' \subseteq S$ *a finite generating set for* G.

Proof. Let R be a finite generating set for G. Every element of R is expressible as a product of elements of S and their inverses. Since R is finite, only finitely many elements of S appear in these expressions; let S' be the set of all such. □

Definition 12. *Let $S \subseteq G$. The* normal closure of S in G *(or the* normal subgroup of G generated by S*) is the smallest normal subgroup of G containing S. It is denoted $\langle\langle S \rangle\rangle^G$.*

Proposition 13. *For any $S \subseteq G$,*

$$\langle\langle S \rangle\rangle^G = \langle S^G \rangle,$$

where $S^G = \{gsg^{-1} : s \in S, g \in G\}$.

Theorem 14. *Let $H \leq_f G$. Then G is finitely generated iff H is.*

Proof. Let T be a transveral to H in G. We may assume $e \in T$. If R is a finite generating set for H, then $S = R \cup T$ is a finite generating set for G.

The converse direction is more involved. Let S be a finite generating set for G. We may assume that for all $s \in S$, $s^{-1} \in S$. Let $R = H \cap \{ts(t')^{-1} : s \in S; t, t' \in T\}$. Then $R \subseteq H$ is finite; we claim that it generates H. Let $h \in H$. Then there exist $s_i \in S$ such that $h = s_1 \cdots s_n$. Define $t_i \in T$ recursively via: $t_0 = e$, and, given t_i, let t_{i+1} be the unique element of T satisfying $H(t_i s) = Ht_{i+1}$ (so that $t_i s t_{i+1}^{-1} \in R$). Then:

$$\begin{aligned} h &= s_1 \cdots s_n \\ &= s_1(t_1^{-1}t_1)s_2(t_2^{-1}t_2)s_3 \cdots s_{n-1}(t_{n-1}^{-1}t_{n-1})s_n \\ &= (t_0 s_1 t_1^{-1})(t_1 s_2 t_2^{-1}) \cdots (t_{n-2}s_{n-1}t_{n-1}^{-1})(t_{n-1}s_n). \end{aligned}$$

Since $h \in H$, $t_{n-1}s_n = t_{n-1}s_n t_0^{-1} \in R$ also, hence $h \in \langle R \rangle$. □

The next Theorem is the only result in this document whose proof is not entirely elementary. The details of the proof will not concern us in this course.

Theorem 15 (Classification of finitely generated abelian groups)**.** *Set G be a finitely generated abelian group. Then there is a finite abelian group T, and $d \in \mathbb{N}$ such that $G \cong \mathbb{Z}^d \times T$. Moreover T is a direct product of cyclic groups.*

Theorem 16 (1st Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a homomorphism of groups. Then $\ker(\phi) \lhd G$, and $G/\ker(\phi) \cong \mathrm{im}(\phi)$.*

Theorem 17 (2nd Isomorphism Theorem)**.** *Let $H \leq G$ and $N \lhd G$. Then $N \cap H \lhd H$, and $H/(N \cap H) \cong HN/N$.*

Theorem 18 (3rd Isomorphism Theorem)**.** *Let $K, N \lhd G$, with $K \leq N$. Then $N/K \lhd G/K$ and $(G/K)/(N/K) \cong G/N$.*

Definition 19. *A homomorphism $\phi : G \to G$ is called an* endomorphism of G*. If ϕ is bijective, then it is called an* automorphism of G.

Proposition 20. *The set* $\mathrm{Aut}(G)$ *of all automorphisms of the group G forms a group under composition of functions, called the* automorphism group of G.

We would like to have some techniques for building new groups from old.

Definition 21 (External semidirect product)**.** *Let Q, N be groups, and let $\phi : Q \to$* $\mathrm{Aut}(N)$ *be a homomorphism. The* (external) semidirect product of N by Q *(with respect to ϕ) is the pair $Q \ltimes_\phi N = \big(Q \times N, \cdot\big)$, where $\cdot$ is the binary operation on $Q \times N$ given by:*

$$(q_1, n_1) \cdot (q_2, n_2) = \big(q_1 q_2, \phi(q_2^{-1})[n_1] n_2\big)$$

Proposition 22. *Under the operation above, $Q \ltimes_\phi N$ is a group. We have $\{e_Q\} \times N \lhd Q \ltimes_\phi N$ and $Q \times \{e_N\} \leq Q \ltimes_\phi N$. Moreover $N \cong \{e_Q\} \times N$ and:*

$$(Q \ltimes_\phi N)/(\{e_Q\} \times N) \cong Q \cong Q \times \{e_N\}.$$

Example 23. *If $\phi : Q \to$* $\mathrm{Aut}(N)$ *is the trivial homomorphism, then $Q \ltimes_\phi N$ is the direct product $Q \times N$ of Q and N.*

Note that there is a potential ambiguity between the notation for the direct product $Q \times N$ (a group) and the Cartesian product $Q \times N$ (a set, which is the underlying set for every external semidirect product of N by Q). We shall always refer to a semidirect product with nontrivial homomorphism ϕ as $Q \ltimes_\phi N$, and never denote it by its underlying set $Q \times N$.

Definition 24 (Internal semidirect product)**.** *Let $Q, N \leq G$. Suppose that:*

(i) $N \lhd G$;

(ii) $Q \cap N = \{e\}$;

(iii) $G = QN = \{qn : q \in Q, n \in N\}$.

Then we call G the (internal) semidirect product of N by Q.

Lemma 25. *Let $N \lhd G$. For $g \in G$, define $c_g : N \to N$ by $c_g(n) = gng^{-1}$. Then $c_g \in$* $\mathrm{Aut}(N)$ *and $g \mapsto c_g$ defines a homomorphism $\Phi : G \to$* $\mathrm{Aut}(N)$.

Proposition 26. *Suppose G is the internal semidirect product of N by Q. Let $\Phi : G \to \mathrm{Aut}(N)$ be as in Lemma 25, and let $\phi = \Phi\,|_H$. Then $(q, n) \mapsto qn$ defines an isomorphism of groups $Q \ltimes_\phi N \cong G$.*

Conversely, for any groups N and Q, and any homomorphism $\phi : Q \to \mathrm{Aut}(N)$, $Q \ltimes_\phi N$ is the internal semidirect product of $\{e_Q\} \times N$ by $Q \times \{e_N\}$.

Definition 27. *For $(G_i)_{i\in I}$ a family of groups indexed by a set I, the* direct product *of the G_i is the set of all ordered tuples $(g_i)_{i\in I}$, with $g_i \in G_i$, denoted:*

$$\prod_{i\in I} G_i$$

and is naturally a group under the operation $(g_i)(h_i) = (g_i h_i)$. The direct sum *of the G_i is:*

$$\bigoplus_{i\in I} G_i = \{(g_i)_{i\in I} : g_i = e \text{ for all but finitely many } i \in I\} \subseteq \prod_{i\in I} G_i$$

The direct sum is clearly a subgroup of the direct product. They are equal iff G_i is trivial for all but finitely many $i \in I$. If $I = \{1, 2\}$, we may write:

$$G_1 \times G_2 = \prod_{i\in I} G_i = \bigoplus_{i\in I} G_i$$

instead. The direct product $Q \times N$ is a special case of the semidirect product of N by Q, corresponding to the trivial homomorphism $\phi : Q \to \mathrm{Aut}(N)$.

Proposition 28. *Identifying G_i with a subgroup of $\bigoplus_{i\in I} G_i$ in the obvious way, and supposing $S_i \subseteq G_i$ with $G_i = \langle S_i \rangle$ for all $i \in I$, we have:*

$$\bigoplus_{i\in I} G_i = \left\langle \bigcup_{i\in I} S_i \right\rangle.$$

Definition 29. *Given groups N and Q, we say a group G is an* extension *of N by Q if there exists $N' \lhd G$ with $N' \cong N$ and $G/N' \cong Q$.*

Example 30. *(i) If G is isomorphic to a semidirect product of N by Q, then it is an extension of N by Q.*

(ii) Both C_4 and $C_2 \times C_2$ are extensions of C_2 by C_2, but C_4 is not isomorphic to a semidirect product of C_2 by C_2.

Proposition 31. *Suppose G is an extension of N by Q.*

(i) If N and Q are finitely generated, then so is G.

(ii) If G is finitely generated, then so is Q.

Remark 32. *If G is an extension of N by Q, and G is finitely generated, it does* not *follow that N is finitely generated (we shall see examples in the course that illustrate this). However if G is finitely generated and Q is finite, then by Theorem 14, N is finitely generated too.*

The following notation is convenient (and widely used) for describing extensions. If G is an extension of N by Q, then there is an injective homomorphism $\iota : N \to G$ and a surjective homomorphism $\pi : G \to Q$ satisfying $\ker(\pi) = \mathrm{im}(\iota)$. We may summarise this data in the following diagram, called a *short exact sequence*:

$$\{e\} \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} Q \longrightarrow \{e\} .$$

To readers unfamiliar with the notion of an "exact sequence" in algebra, the presence of the trivial group in the above diagram may seem superfluous. We shall not comment on the reason for its inclusion here, and just accept it as a notational convention.

In what follows, $\mathcal{P}$ and $\mathcal{Q}$ are properties fo groups (for example "finite", "abelian", "cyclic" etc.).

Definition 33. *We say a group G is $\mathcal{P}$*-by-*$\mathcal{Q}$ if there exist groups N and Q such that N is $\mathcal{P}$; Q is $\mathcal{Q}$ and G is an extension of N by Q.*

Definition 34. *We say that the group G* virtually *has the property $\mathcal{P}$ (or sometimes just, G* is *virtually $\mathcal{P}$) if there exists $H \leq_f G$ such that H is $\mathcal{P}$.*

Proposition 35. *Suppose that $\mathcal{P}$ is a property of groups which is inherited by finite-index subgroups (that is, if G is $\mathcal{P}$ and $H \leq_f G$ then H is $\mathcal{P}$). Suppose that G is virtually $\mathcal{P}$. Then G is $\mathcal{P}$-by-finite.*

Proof. This is immediate from the definitions and Proposition 7. □

We now turn, briefly, away from groups and to metric spaces.

Definition 36. *A* metric space *is a pair (X, d), where X is a nonempty set and d is a function $X \times X \to [0, \infty)$ satisfying, for all $x, y, z \in X$,*

(i) $d(x, y) = 0$ iff $x = y$;

(ii) $d(x, y) = d(y, x)$*;*

(iii) $d(x, z) \leq d(x, y) + d(y, z)$ *(the* triangle inequality*).*

Such a function called a metric *on* X.

Informally, $d(x, y)$ measures the "distance" between the points x and y in X. Henceforth let (X, d) be a metric space.

Definition 37. *A subset* $U \subseteq X$ *is* open *if, for every* $u \in U$*, there exists* $\epsilon > 0$ *(depending on u) such that, for all* $x \in X$*, if* $d(u, x) < \epsilon$ *then* $x \in U$.

Proposition 38. *Let* (X, d) *be a metric space.*

(i) X *and* $\emptyset$ *are open;*

(ii) If $U, V \subseteq X$ *are open, then so is* $U \cap V$*;*

(iii) If $(U_i)_{i \in I}$ *is a family of open sets, then* $\bigcup_{i \in I} U_i$ *is open.*

Thus the metric space (X, d) naturally has the structure of a *topological space*.

Definition 39. *A subset* $C \subseteq X$ *is* closed *if, whenever* (c_n) *is a sequence of points in* C *and* $x \in X$*, if* $d(x, c_n) \to 0$ *as* $n \to \infty$*, then* $x \in C$.

Proposition 40. *The subset* $C \subseteq X$ *is closed iff* $X \setminus C$ *is open.*

Definition 41. *A point* $x \in X$ *is* isolated *if* $\{x\} \subseteq X$ *is open.*

By Proposition 40, $x \in X$ is isolated iff there is no sequence of points (x_n) in X such that $d(x, x_n) \to 0$ as $n \to \infty$.