Some Very Incomplete
Introductory Notes on Group Theory

Laurence Barker, 30 December 2016, Bilkent University.

It is perhaps unlikely that I will ever be in a position to change the title to "Some Incomplete Notes in Group Theory". Nevertheless, I leave some spaces so that more can be inserted later.

1: Introduction

History, symmetries of equations, symmetries of mathematical objects.

2: Some language from set theory

Intersection. Functions. Equivalence relations.

2: Some classical number theory

Euclidian algorithm. Fermat's Little Theorem. Warm up for Lagrange's Theorem by proving Euler's Little Theorem using the method in the proof of Lagrange.

3: Matrices of degree 2

Just 2×2 matrices over $\mathbb{Q}$ and $\mathbb{R}$ and $\mathbb{C}$. Include determinants, representation of quaternions, sum of four squares.

4: The definition of a group

Write operation as $*$. Uniqueness of identity and reverse. Define isomorphism. Classify, up to isomorphism, groups of order at most 7.

5: Some fundamental properties of abelian groups

FISH.

5.1: Orders of subgroups of finite abelian groups

5.2: The abelian group cases of the Three Isomorphism Theorems

Theorem: (First Isomorphism Theorem for Abelian Groups.) *Let A and B be abelian groups and let $\theta : A \to B$ be a homomorphism. Then $\theta(A)$ is a subgroup of B and $A/\ker(\theta) \cong B$.*

Theorem: (Second Isomorphism Theorem for Abelian Groups.) *Let B and C be subgroups of an abelian group A. Then $B/(B \cap C) \cong (B + C)/C$.*

Theorem: (Third Isomorphism Theorem for Abelian Groups.) *Let $C \leq B \leq A$ be abelian groups. Then $(A/C)/(B/C) \cong A/B$.*

Chinese Remainder Theorem.
Nilpotency of abelian groups.

6: Similar fundamental properties for arbitrary groups

Use multiplicative notation.

6.1: Lagrange's Theorem

Consider a subgroup H of a group G. Given $g \in G$, the set

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

is called a **left coset** of H in G.

Proposition: *Given groups $H \leq G$, then G is the disjoint union of the left cosets of H in G.*

Proof: Given $g \in G$, then $g \in gH$. So, letting g run over the elements of G, the union of the subsets gH is G. It remains to show that any two distinct left cosets of H in G are disjoint. Let $f, g \in G$ and suppose that $fH \cap gH \neq \emptyset$. We must show that $fH = gH$. Choose an element $x \in fH \cap gH$. Then $fu = x = gv$ for some $u, v \in H$. Given $h \in H$, then $fh = gvu^{-1}h$ and $vu^{-1}h \in H$, hence $fH \subseteq gH$. A similar argument shows that $fH \supseteq gH$. Therefore $fH = gH$, as required. $\square$

The set Hg is called a **right coset** of H in G. Plainly, an assertion similar to the latest proposition holds for the right cosets of H in G.

Theorem: (Lagrange's Theorem.) *Given a finite group G and $H \leq G$, then $|H|$ divides $|G|$.*

Proof: The function $H \to gH$ given by $H \ni h \mapsto gh$ is bijective, indeed, the inverse is plainly given by $g^{-1}k \hookleftarrow k \in K$. Therefore, $|H|$. In view of the previous proposition, $|G|$ must be equal to $|H|$ times the number of left cosets of H in G. $\square$

6.2: The Three Isomorphism Theorems

Theorem: (First Isomorphism Theorem.) *Given a group homomorphism $\theta : G \to H$, then* $\ker(\theta) \trianglelefteq G$ *and* $\theta(G) \leq H$ *and*

$$G/\ker(\theta) \cong \theta(H) \ .$$

Writing $K = \ker(\theta)$, there is an isomorphism $G/K \to \theta(H)$ given by $gK \mapsto \theta(g)$ for $g \in G$.

Proof: Given $k, k' \in K$, then $kk' \in K$ because $\theta(kk') = \theta(k)\theta(k') = 1$. Similarly, $k^{-1} \in K$. So $K \leq G$. Given $g \in G$, then $\theta(gkg^{-1}) = \theta(g)\theta(k)\theta(g^{-1}) = \theta(g)\theta(g)^{-1} = 1$. So $K \trianglelefteq G$. Another routine argument, again demonstrating closure under multiplication and inversion, shows that $\theta(G) \leq H$.

The function $\Theta : G/K \to \theta(H)$ given by $\Theta(gK) = \theta(g)$ is well-defined and injective because, for $f, g \in G$, the condtion $fK = gK$ and the condition $\theta(F) = \theta(g)$ are plainly both equivalent to the condtion $f^{-1}g \in K$. $\square$

Theorem: (Second Isomorphism Theorem.) *Given finite groups $H \leq G \trianglerighteq K$, then $H \cap K \trianglelefteq H$ and $K \trianglelefteq HK \leq G$ and*

$$H/(H \cap K) \cong HK/K \ .$$

There is an isomorphism $H/(H \cap K) \to HK/K$ given by $h(H \cap K) \mapsto hK$ for $h \in H$.

Proof: Consider elements $x, x' \in HK$. To show that $HK \leq G$, we must show that $xx' \in HK$ and $x^{-1} \in HK$. Write $x = hk$ and $x' = h'k'$ with $h, h' \in H$ and $k, k' \in K$. The normality of K

implies that $Kh' = h'K$. Hence $kh' = h'k''$ for some $k'' \in K$. Therefore $xy = hkh'k' = hh'k''k'$. But $hh' \in H$ and $kk' \in K$, hence $xx' \in HK$. A similar argument shows that $x^{-1} \in HK$. We have confirmed that $HK \leq G$.

Trivially, $K \trianglelefteq HK$. Let $\theta : H \to HK/K$ be the function such that $\theta(h) = hK$ for $h \in H$. We have $\theta(h)\theta(h') = hK.h'K = hh'K = \theta(hk)$. Therefore θ is a homomorphism. Noting that $hkK = hK$, we see that θ is surjective. Since $\ker(\theta) = \{h \in H : hK = K\} = H \cap K$, the First Isomorphism Theorem tells us that $H \cap K \trianglelefteq H$ and that there is an isomorphism as specified. □

Theorem: (Third Isomorphism Theorem.) *Let $H \trianglelefteq G \trianglerighteq K$ with $K \leq H$. Then $K \trianglelefteq H$ and $H/K \trianglelefteq G/K$ and*

$$(G/K)/(H/K) \cong G/H \ .$$

Proof: Plainly, $K \trianglelefteq H$. Let $f, g \in G$. If $f^{-1}g \in K$ then $f^{-1}g \in H$. That is to say, if $fK = gK$ then $fH = gH$. So there is a well-defined function $\theta : G/K \to G/H$ given by $gK \mapsto gH$. It is easy to see that θ is a homomorphism. The kernel of θ is $\{hK : h \in H\} = H/K$.

6.3: The Direct Product Recognition Theorem

foxcat

7: Permutation sets

Orbit-Stabilizer Equation.

8: Sylow's Theorem

This is a *Snow Emergency Discussion of Sylow's Theorem*, written on 30 December. It is an account for those who, due to decorative but impractical weather, were unable to attend the last two hours of lectures. Since the day includes four hours of lectures, two meetings with research students, plus other small jobs, the following is composed very fast, and will probably have some mistakes and substantial omissions.

Throughout, we let p be a prime. Below, we shall give a general definition of the notion of a p-group. As we mentioned in earlier lectures, it will turn out that a finite group G is a p-group if and only if $|G|$ is a power of p. For the time-being, we consider only finite groups, taking that necessary and sufficient condition as the definition of the term.

A subgroup $P \leq G$ is called a **p-subgroup** of G provided P is a p-group.

Write $|G| = p^a m$ where a is a natural number and m is a positive integer coprime to p. A subgroup $P \leq G$ is called a **p-subgroup** of G provided P is a p-group, equivalently, $|P|$ divides p^a. When $|P| = p^a$, we call P a **Sylow p-subgroup** of G.

In earlier lectures, we showed that finite p-groups have the following two remarkable properties. Those and some other some other properties of p-groups provide part of the initial motivation for a study of the p-subgroups of G.

Theorem 8.1: *Given a non-trivial finite p-subgroup P, then $Z(P)$ is non-trivial.*

Theorem 8.2: *Given finite p-groups $Q < P$, then $Q < N_P(Q)$.*

We showed, recall, how Theorem 8.2 follows from Theorem 8.1 which, in turn, follows from the next lemma. Some more notation is needed to express the lemma. Given a G-set X and

an element $x \in X$ such that $gx = x$ for all $g \in G$, then we say that x is **fixed** by G. We write X^G to denote the subset of X consisting of those elements which are fixed by G.

Lemma 8.3: *Let P be a finite p-group and X a finite P-set. Then $|X| \equiv |X^P|$ modulo p.*

The following Theorem was given by Peter Ludwig Mejdell Sylow in a 10-page paper published in 1872. The main content of the theorem, we mean to say, the main difficulty in proving it, is in establishing the existence of a Sylow p-subgroup. In the first proof we supply, the the quick proof of existence was found by Helmut Wielandt in, I think, the 1930s.

Theorem 8.4: (Sylow's Theorem) *Let p be a prime and G a finite group. Write $|G| = p^a m$ where a is a natural number and m is a positive integer not divisible by p. Then:*
Maximality: *Every p-subgroup of G is contained in some Sylow p-subgroup of G.*
Uniqueness: *The Sylow p-subgroups of G are mutually G-conjugate.*
Enumeration: *The number $s_p(G)$ of Sylow p-subgroups of G is congruent to 1 modulo p, also, $s_p(G)$ divides m.*

Proof: Let $\mathcal{W}$ be the set of subsets $W \subseteq G$ such that $|W| = p^a$. We make G act on $\mathcal{W}$ by left multiplication, we mean, an element $g \in G$ sends an element $W \in \mathcal{W}$ to the element $gW = \{gw : w \in W\} \in \mathcal{W}$. By the definition of binomial coefficients,

$$|\mathcal{W}| = \binom{p^a m}{p^a} = \frac{p^a m}{p^a} \cdot \frac{p^a m - 1}{p^a - 1} \cdots \frac{p^a m - p^a + 2}{2} \cdot \frac{p^a - p^a + 1}{1} .$$

For each ratio $(p^a m - r)/(p^a - r)$ appearing in the product, the largest power of p dividing the numerator is equal to the largest power of p dividing r, which is also equal to the highest power of p dividing the denominator. Therefore, $|\mathcal{W}|$ is coprime to p. So some G-orbit $[W]_G$ in $\mathcal{W}$ is coprime to p. Replacing W by another element in the same G-orbit if necessary, we may assume that $1 \in W$. That condition implies that W contains the stabilizer S of W in G. In particular, $|S| \leq |W| = p^a$. On the other hand, the Orbit-Stabilizer Equation says that, $|G| = |S||[W]_G|$. Hence p^a divides $|S|$. Those two conditions on $|S|$, together with the obvious inequality $1 \leq |S|$, yield $|S| = p^a$, in other words, the subgroup S is a Sylow p-subgroup of G.

Let $\mathrm{Syl}_p(G)$ denote the set of Sylow p-subgroups of G. The achievement of the previous paragraph was to demonstrate that $\mathrm{Syl}_p(G) \neq \emptyset$. Our next main step is to show that the positive integer $s_p(G) = |\mathrm{Syl}_p(G)|$ is congruent to 1 modulo p. Consider an arbitrary p-subgroup P of G. We let P act on $\mathrm{Syl}_p(G)$ by conjugation, any $u \in P$ sending any TıSyl$_p(G)$ to ${}^uP \in \mathrm{Syl}_p(G)$. Lemma 8.3 says that $s_p(G) \equiv |\mathrm{Syl}_p(G)^P|$ modulo p.

We claim that, given $T \in \mathrm{Syl}_p(G)$, then $T \in \mathrm{Syl}_p(G)^P$ if and only if $P \leq T$. In one direction, this is clear. Conversely, suppose that $T \in \mathrm{Syl}_p(G)^P$, in other words, $P \leq N_G(T)$. Applying the Second Isomorphism Theorem to the subgroups $P \leq N_G(T) \trianglerighteq T$, we deduce that $PT \leq G$ and $PT/T \cong P/(P \cap T)$. Hence

$$|PT|/|T| = |P|/|P \cap T| .$$

By Lagrange's Theorem, the right-hand side of that equality is a power of p. Therefore $|PT|$ is a power of p divisible by the integer $|T| = p^a$. But, by Lagrange's Theorem again, $|PT|$ divides $|G|$. So $|PT| = |T|$ and $|P| = |P \cap T|$, hence $P \leq T$. The claim is established.

Putting $P = S$, we have $S \leq T$ if and only if $S = T$. By the claim, $\mathrm{Syl}_p(G)^S = \{S\}$. Therefore $s_p(G) = |\mathrm{Syl}_p(G)^S| = |\{S\}| = 1$.

Now let P be arbitrary. Since $s_p(G)$ is coprime to p, some P-orbit of $\mathrm{Syl}_p(G)$ must be a singleton set $\{T\}$. By the claim again, $P \leq T$. Demonstration of the Maximality part is now complete.

Write $\mathrm{Syl}_p(G) = A \sqcup B$, a disjoint union, where A and B are unions of G-orbits. If A is non-empty then, choosing any $T \in A$, the equality $\mathrm{Syl}_p(G)^T = \{T\}$ implies that $|A| \equiv 1$ and $|B| \equiv 0$. Similarly, if B is non-empty, then $|A| \equiv 0$ and $|B| \equiv 1$. This is a contradiction, unless $A = \emptyset$ or $B = \emptyset$. We have shown that the G-set $\mathrm{Syl}_p(G)$ is transitive. The Uniqueness part is now finished.

Finally, by the Uniqueness part and the Orbit-Stabilizer Equation, $s_p(G) = |G : N_G(S)|$, which evidently divides the integer $|G : S| = m$. $\square$

During a lecture in 1862, ten years before the publication of his theorem, Sylow raised the following question:

Sylow's 1862 question: *Given a finite group G and a natural number b such that p^b divides $|G|$, must G have a subgroup of order p^b?*

The question was linked to a now somewhat obsolete theorem of Cauchy asserting that, if p divides $|G|$, then G has an element of order p. To put it another way, Cauchy's Somewhat Obsolete Theorem says that the affirmative answer to the above question is correct when $b = 1$.

Corollary 8.5: *The affirmative answer to Sylow's 1862 question is correct.*

Proof: This follows from Sylow's Theorem together with the next lemma. $\square$

Lemma 8.6: *Let P be a finite p-group and b a natural number such that p^b divides P. Then P has a subgroup with order p^b.*

We leave the proof of that lemma as an exercise. Hint: Use Theorem 8.1 and an inductive argument on $|P|$.

Corollary 8.7: *Let P be a finite group. Then P is a p-group if and only if, for every element $g \in P$, the order of g is a power of p.*

Proof: If $|P|$ is a p-group, then Lagrange's Theorem immediately implies that, for every element, the order is a power of p. Conversely, suppose that P is not a p-group. Let q be a prime divisor of $|G|$ distinct from p. By Corollary 8.5 (or just by Cauchy's Somewhat Obsolete Theorem), P has an element of order q. $\square$

An arbitrary group G, possibly infinite, is called a **p-group** provided, for all $g \in G$, there exists a natural number a such that $g^{p^a} = 1$. The latest corollary ensures that, in the special case of finite G, this definition is equivalent to the one we gave before.

We point out that, for such G, there need not exist a natural number a such that, for all $g \in G$, we have $g^{p^a} = 1$. An example to show the need to take care over the quantifiers is the Prüfer p-group C_{p^∞}. As one construction, C_{p^∞} can be regarded as the multiplicative group of complex numbers having the form $e^{2\pi ni/p^a}$ where $n \in \mathbb{Z}$ and $a \in \mathbb{N}$. Another isomorphic copy of C_{p^∞} is the quotient group $\mathbb{Z}_{(p)}/\mathbb{Z}$, under addition, where $\mathbb{Z}_{(p)}$ is the set of p-local integers, we mean, rational numbers having the form n/p^a with n and a as before.

Standard Kind of Application of Sylow's Theorem Question: Let G be a simple group of order 504. Suppose that G is not isomorphic to a subgroup of A_8. How many Sylow 7-subgroups does G have?

Solution: By Sylow's Theorem, the number s of such subgroups is congruent to 1 modulo 7 and divides the number $504/7 = 72 = 8.9$. The divisors of 8.9 are 1, 2, 4, 8, 3, 6, 12, 24, 9, 18, 36, 72. So $s \in \{1, 8, 36\}$. If $s = 1$ then G has a normal Sylow 7-subgroup, which is impossible because G is simple. Suppose, for a contradiction, that $s = 8$. Then there exists a non-trivial homomorphism $\theta : G \to S_8$. Since G is simple, θ is injective. The hypothesis on G implies that $\theta(G) \not\leq A_8$. Hence $A_8 \cap G$ is a normal subgroup of G with index 2. Again, this contradicts the simplicity of G. Therefore, $s = 36$.

Comment: Up to isomorphism, there is exactly one simple group of order 504. It is the group $\mathrm{SL}_2(8)$ of 2×2 matrices A with entries in the field of order 8 and such that the determinant of A is 1.