CMSC 36500 / MATH 37500 Algorithms in Finite Groups

Instructor: László Babai
Scribe: Robert Green

Spring 2017

2 Lecture 2 March 30, 2017 Problems due April 4

2.1 Homework review

We will discuss a few of the homework problems from last time:

Review 2.1. *If G is abelian and characteristically simple then G is elementary abelian (i.e. $\mathbb{Z}_p^k$ for some p prime and k positive integer)*

Proof. Suppose p is a divisor of $|G|$ and we write G additively. Then look at $p \cdot G := \{px \mid x \in G\}$. Note that pG is characteristic in G and $pG \neq G$ (since the elements of order p are in the kernel of the $x \mapsto px$ homomorphism). Since G is characteristically simple, $pG = 0$. Now apply the Fundamental Theorem of Finite Abelian Groups. □

Review 2.2. *If $M \overset{\min}{\lhd} G$ then M is characteristically simple.*

Proof. Any characteristic subgroup N of M is normal in G and therefore either $N = M$ or N is trivial. □

DO 2.3. *Let G be solvable. Then for all $H \leq G$ we have H is solvable, and for every $N \lhd G$, we have G/N is solvable.*

Review 2.4. *If G is solvable and $M \overset{\min}{\lhd} G$, then M is elementary abelian.*

Proof. M' (the commutator subgroup of M) is characteristic and therefore either $M' = M$ or $M' = 1$ (because M is characteristically simple). $M' = M$ would imply that M is not solvable, contradicting the solvability of G, so $M' = 1$, i.e., M is abelian. Now M is abelian and characateristicaly simple, therefore elementary abelian by Review 2.1. □

DO 2.5. *Transpositions generate S_n and three-cycles generate A_n.*

Review 2.6. *A_n is the only subgroup of index two in S_n.*

Proof. First we make some general observations about any group G and a subgroup H of index 2. We note that $H \lhd G$ (since $G \setminus H$ is the only coset other than H, whether right coset or left coset). So there is an epimorphism $\varphi : G \to G/H \cong \{\pm 1\}$ where $\{\pm 1\}$ is a convenient way to think about the cyclic group of order 2 under multiplication. By definition, the kernel of φ is H. We note that $(\forall x \in H)(x^2 \in \ker \varphi)$ because $\varphi(x^2) = (\varphi(x))^2 = (\pm 1)^2 = 1$. So $H \geq \langle x^2 \mid x \in G \rangle$.

Now for $G = S_n$ let $K = \langle x^2 \mid x \in S_n \rangle$. We claim $K = A_n$. Indeed, let $\sigma \in S_n$ be a 3-cycle. Then $\sigma^3 = 1$ and therefore $\sigma = \sigma^4 = (\sigma^2)^2$, so $\sigma \in K$. So all 3-cycle belong to K. But the 3-cycles generate A_n, so $K \geq A_n$. In fact $K = A_n$ (why?).

We proved that $H \geq A_n$. But $|S_n : H| = |S_n : A_n| = 2$, so $H = A_n$. □

Alternatively, there is a quick way to prove this for $n \geq 5$ by noting that A_n is simple, so the existence of another (necessarily normal) subgroup N of index two implies that $A_n \cap N$ is normal in A_n, contradicting simplicity of A_n. (However, the proof above is from first principles, and settles all cases.)

Review 2.7. *If $G \leq S_{p^k}$ and G is transitive, then for $P \in Syl_p(G)$ we have that P is transitive.*

Proof. We observe that $|G : G_x| = |x^G| = p^k$. We must show that $|x^P| = p^k$. Clearly, $|x^P| \leq p^k$, so we need to show $|x^P| \geq p^k$, i.e., $|P : P_x| \geq p^k$, i.e., $|P_x| \leq \frac{|P|}{p^k}$.

Let G have order $p^\ell \cdot m$ where p and m are coprime. It follows that $p^\ell = |P|$, so we need to show that $|P_x| \leq p^{\ell-k}$. But $|G_x| = |G|/p^k = p^{\ell-k}m$, and P_x is a p-subgroup of G_x, so the order of P_x divides $p^{\ell-k}$. □

2.2 Generators, group extensions, solvability

DO 2.8. *If G is not abelian then $G/Z(G)$ is not cyclic. (Note: this problem was erroneously stated in class, with G' in place of $Z(G)$. Show that this statement is false.)*

HW 2.9. *If $|G| = n$ then G can be generated by at most $\log_2(n)$ elements.*

HW 2.10. *(a) If $|G| = n$ then $|Aut(G)| \leq n^{\log_2(n)}$ with equality holding if and only if G is trivial. (b) Prove that this bound is tight up to a constant factor for infinitely many values of n. In other words, find a constant $c > 0$ and for infinitely many n, find G of order n such that $|Aut(G)| > c \cdot n^{\log_2(n)}$.*

Definition 2.11 (Group extension)**.** *Suppose $N \lhd G$ and $H = G/N$. Then we say that "**G is an extension of N by H**". In category-theoretic notation, we write*

$$1 \to N \to G \to H \to 1$$

and say that this is an "exact sequence," meaning that the image at the head of every arrow is the kernel at the tail of the next arrow.

DO 2.12 (Solvable groups are closed under extension)**.** *If N and H are solvable and G is an extension of N by H, then G is solvable.*

DO 2.13. *S_n and $A_n \times \mathbb{Z}_2$ are extensions of A_n by $\mathbb{Z}_2$. Prove that for $n > 2$ these two groups are not isomorphic. In particular, extensions are not unique.*

DO 2.14. *Find a nonabelian extension of $\mathbb{Z}_7$ by $\mathbb{Z}_3$*

DO 2.15. *No nonabelian extension of $\mathbb{Z}_5$ by $\mathbb{Z}_3$ exists.*

DO 2.16. *In fact, if G is abelian and $|G|$ is square-free, then G is cyclic.*

DO 2.17. *S_n is solvable for $n \leq 4$, and S_n is not solvable for $n \geq 5$.*

Theorem 2.18 (Feit–Thompson Theorem (1963), aka the "Odd-Order Theorem")**.**
If $|G|$ is odd then G is solvable.

Definition 2.19 (Normal closure)**.** *Consider $S \subseteq G$. Then $NCl_G(S)$ is the smallest normal subgroup of G containing S. It is generated by the union of all conjugates of S.*

DO 2.20. *Let G be generated by S. Then $G' = NCl_G([x, y] \mid x, y \in S)$.*

2.3 Nilpotent groups

Definition 2.21 (Mutual commutator of two subgroups)**.** *For $A, B \leq G$, we define*

$$[A, B] := \langle [a, b] \mid a \in A, b \in B \rangle$$

DO 2.22. *Let $G' = [G, G]$ be the commutator subgroup of G.*

(a) G/G' is abelian

(b) G' is the smallest normal subgroup N such that G/N is abelian, i.e., if $N \lhd G$ and G/N is abelian then $N \geq G'$.

Definition 2.23 (Lower central series (aka "descending central series"))**.**

$$L^0(G) = G \text{ and } L^i(G) = [L^{i-1}(G), G]$$

DO 2.24. $G = L^0(G) \geq L^1(G) \geq L^2(G) \geq \ldots$

DO 2.25. $L^i(G)$ char G

Definition 2.26 (Nilpotence class)**.** *G is nilpotent if there exists k so that $L^k(G) = 1$. G is nilpotent of class k if k is the smallest such number.*

DO 2.27. *G is nilpotent of class 1 if and only if G is abelian. G is nilpotent of class 2 if and only if $G' \leq Z(G)$.*

Problem 2.28 (Group Isomorphism problem)**.** *Given G and H, decide if $G \cong H$.*

A question arises here as to how the group is represented. If it is presented in terms of generators and relations, then whether or not the group is trivial is already undecidable. So let's be generous: suppose we are given the Cayley table (multiplication table) of G and H.

HW 2.29. *Suppose $|G| = |H| = n$. Give an algorithm to decide whether or nor $G \cong H$ in time $n^{\log_2(n)+c}$.*

Theorem 2.30 (F. Wagner, D. Rosenbaum)**.** *Group isomorphism can be decided in time*

$$n^{(\log_2 n)/4+c}$$

.

OPEN PROBLEM 2.31. *Decide group isomorphism in time $n^{o(\log(n))}$ for nilpotent groups of class 2.*

Definition 2.32 (Upper (ascending) central series)**.**

$$Z_0(G) = 1 \text{ and } Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$$

DO 2.33. $Z^i(G)$ char G. *Therefore $Z^i(G) \lhd G$. Therefore the above inductive definition makes sense.*

DO 2.34. $1 = Z^0(G) \leq Z^1(G) \leq L^2(G) \leq \ldots$

DO 2.35. $L^k(G) = 1 \iff Z_k(G) = G$. *In particular, G is nilpotent if and only if the upper central series reaches G, and the nilpotence class of G is the smallest k such that $Z_k(G) = G$.*

DO 2.36. *If G is a nontrivial finite p-group then $Z(G)$ is nontrivial. It follows that finite p-groups are nilpotent.*

DO 2.37. *Nilpotent groups are closed under taking subgroups, quotients, and finite direct products, but not under extensions.*

HW 2.38. *Find the smallest group G such that G is an extension of a nilpotent group by a nilpotent group but G is not nilpotent.*

DO 2.39. *If G is nilpotent then G is solvable. The converse is false; find the smallest counterexample.*

Theorem 2.40 (Philip Hall)**.** *If G is nilpotent of class k with derived length d, then $d \leq 1 + \log_2(k)$*

DO 2.41. *G is nilpotent $\iff$ all Sylow subgroups are normal $\iff$ G is a direct product of its Sylow subgroups.*

DO 2.42. *Consider $M(d,p)$, the p-group of upper triangular $d \times d$ matrices over $\mathbb{F}_p$ where all diagonal elements are 1. Show that $|M(d,p)| = p^{\binom{d}{2}}$ and the class of $M(d,p)$ is $d-1$.*

2.4 Primitive permutation groups

Definition 2.43 (System of imprimitivity)**.** *Let $G \curvearrowright \Omega$ be a transitive action of a group G on a set Ω. Let R be a G-invariant equivalence relation on Ω, i.e., $R^G = R$. The equivalence classes of such a relation are called* blocks of imprimitivity*, and the partition (set of blocks) is called a* system of imprimitivity*. A system of imprimitivity is* trivial *if either there is just one block, $|\Omega|$, or each block is a singleton (discrete partition).*

Example 2.44. *Consider D_6, the dihedral group of order 12, acting on the vertices of the regular hexagon. Two nontrivial systems of imprimitivity are the set of opposite pairs of the hexagon (3 blocks), and the two triangles whose vertices are two edges apart (2 blocks).*

Definition 2.45. *We say that a group action is* imprimitive *if there exists a nontrivial system of imprimitivity. An action is* primitive *if $|\Omega| \geq 2$ and the action is not imprimitive, i.e., the action has exactly two (trivial) systems of imprimitivity. We say that a permutation group $G \leq Sym(\Omega)$ is (im)primitive if its action as a subgroup of $Sym(\Omega)$ is (im)primitive.*

HW 2.46. *Let $G \curvearrowright \Omega$ be a transitive action on a set Ω of size $|\Omega| \geq 2$. Prove: this action is primitive $\iff G_x \overset{\max}{<} G$ (G_x is a maximal subgroup of G, i.e., $G_x \neq G$ and if $G_x \leq H \leq G$ then $H = G_x$ or $H = G$).*

Definition 2.47 (Induced action of S_n on k-tuples)**.** *S_n acts naturally on $\binom{n}{k}$ elements (corresponding to the k-subsets of the $[n]$). We denote the permutation group definde by this action by $S_n^{(k)}$, so $S_n^{(k)} \leq S_{\binom{n}{k}}$.*

HW 2.48. *Prove: $S_n^{(k)}$ is primitive for $1 \leq k < n/2$ and imprimitive for $k = n/2$.*