CMSC 36500 / MATH 37500 Algorithms in Finite Groups

Instructor: Laszlo Babai
Notes by Robert Green

Spring 2017

NOTATION:

1. $[n]$ denotes $\{1, \ldots, n\}$
2. **CFSG**: Classification of finite simple groups
3. The trivial group is the group consisting only of the identity element
4. $h^g = g^{-1}hg$ denotes the **conjugate** of h by G
5. $[g, h] = g^{-1}h^{-1}gh$ denotes the commutator of g and h
6. For $S \subseteq G$, $\langle S \rangle$ denotes the subgroup of G generated by S
7. G' denotes the commutator subgroup of G – the subgroup of G generated by all commutators.
8. $Aut(G)$ denotes the group of automorphisms of G
9. $PSL(d, \mathbb{F}) = SL(d, \mathbb{F})/Z(SL(d, \mathbb{F}))$
10. $G \curvearrowright \Omega$ denotes an action of G on the set Ω
11. x^g denotes the action of g on x
12. Stabilizer of $x \in \Omega$ in G under G-action on Ω is denoted $G_x = \{g \in G \mid x^g = x\}$
13. $Syl_p(G)$ denotes the set of Sylow p-subgroups of G
14. $Sym(\Omega)$: the symmetric group on Ω $\quad S_n = Sym([n])$
15. $Alt(\Omega)$: the alternating group on Ω $\quad A_n = Alt([n])$

1 Lecture 1 March 28, 2017

1.1 Some Preliminaries

DO 1.1. *If τ is a (reflection/rotation by α) of $\mathbb{R}^2$ or $\mathbb{R}^3$, and σ is any congruence of the space, then τ^σ is also a (reflection/rotation by $\pm\alpha$), respectively.*

HW 1.2. *Prove: $Inn(G) \lhd Aut(G)$.*
Notation: the outer automorphism group *of G is $Out(G) := Aut(G)/Inn(G)$.*

DO 1.3. *$Z(G)$ and G' are normal in G.*

DO 1.4. *Find the smallest pair (G, H) such that H is a normal subgroup that is not characteristic.*

HW 1.5. *Being a normal subgroup is not a transitive relation. Find the smallest counterexample.*

Definition 1.6. *The symmetric group acting on Ω is denoted $Sym(\Omega)$ and the symmetric group acting on $[n]$ is denoted S_n.*

Definition 1.7. *Let $\mathbb{F}$ be a field and let n be a positive integer. The general linear group $GL(n, \mathbb{F})$ is the group of nonsingular $n \times n$ matrices with entries in $\mathbb{F}$*

DO 1.8. *$Z(S_n)$ is trivial for $n > 2$*

DO 1.9. *$Z(GL(d, \mathbb{F}))$ consists of nothing besides the set of nonzero scalar matrices (scalar multiples of the identity).*

Definition 1.10. *The order of an element g, denoted by $|g|$, is the smallest n so that $g^n = 1$ (where "1" denotes the identity element). Equivalently the order of g is the order of the cyclic subgroup generated by g.*

Definition 1.11. *For a prime p, a p-group is a group whose elements are all of order a power of p.*

DO 1.12. *If G is finite, then G is a p-group if and only if $|G|$ is a power of the prime p.*

DO 1.13. *If G is a finite nontrivial p-group, then $Z(G)$ is nontrivial*

DO 1.14. *Find an epimorphism (surjective homomorphism) $GL(d, \mathbb{F}) \longrightarrow \mathbb{F}^{\times}$*

Definition 1.15. *An even permutation is the product of an even number of transpositions, and an odd permutation is the product of an odd number of transpositions. Check that this is well-defined, i.e., no permutation is simultaneously even and odd.*

DO 1.16. *For $n \geq 2$, $|S_n : A_n| = 2$*

HW 1.17. *A_n is the only subgroup of index two in S_n.*

DO 1.18. *A_n char S_n*

Definition 1.19. *A group is simple if it contains no nontrivial normal subgroups.*

Theorem 1.20. *For $n \geq 5$, A_n is simple.*

Definition 1.21. *The special linear group $SL(d, \mathbb{F})$ is the set of $d \times d$ matrices over $\mathbb{F}$ with determinant 1*

DO 1.22. $SL(d, \mathbb{F}) = GL(d, \mathbb{F}) \iff \mathbb{F} = \mathbb{F}_2$

DO 1.23. $SL \triangleleft GL$

DO 1.24. $Z(SL) = Z(GL) \cap SL$

DO 1.25. $|Z(GL(d, \mathbb{F}_q))| = q - 1$. *Find* $|Z(SL(d, \mathbb{F}_q))|$

DO 1.26. *G is a simple abelian group if and only if $G \cong \mathbb{Z}_p$ for some prime p.*

Definition 1.27. *G is characteristically simple if G has no characteristic subgroup other than G and the trivial group.*

DO 1.28. *Let $T_1, ..., T_k$ be nonabelian simple groups. Count the normal subgroups $N \triangleleft T_1 \times ... \times T_k$. (Hint: the number is 2^k. Prove!)*

Definition 1.29. *An elementary abelian p-group is a group of the form $\mathbb{Z}_p^k$*

DO 1.30. *If T is a simple group, then T^k is characteristically simple.*

DO 1.31. *Prove the converse: if a finite group is characteristically simple then it is the direct product of isomorphic simple groups.*

Definition 1.32. *$N \lhd G$ is a minimal normal subgroup if $N \neq 1$ is normal in G and contains no other normal subgroups except the identity. We denote this by $N \overset{\min}{\lhd} G$.*

DO 1.33. *$G \overset{\min}{\lhd} G \iff G$ is simple.*

DO 1.34. *If $N \overset{\min}{\lhd} G$ then N is characteristically simple.*

The two smallest nonabelian simple groups are A_5 and $PSL(3, \mathbb{F}_2) \cong PSL(2, \mathbb{F}_7)$

DO 1.35. *The set of upper triangular matrices over a fixed finite field of characteristic p form a p-group.*

Definition 1.36. *The commutator chain is a chain of commutator subgroups*

$$G \geq G' \geq G'' \geq ...$$

Definition 1.37. *G is solvable if its commutator chain terminates at the trivial group*

Theorem 1.38. ***(Schreier's Hypothesis)*** *If G is finite simple then $Out(G)$ is solvable. (This is a consequence of* ***CFSG****).*

DO 1.39. *If G is finite then G is solvable $\iff$ all composition factors of G are abelian (i.e. cyclic of prime order).*

Definition 1.40. *A normal chain is a chain of subgroups*

$$G = H_0 \geq H_1 \geq ... \geq H_m = \{e\}$$

where $H_i \lhd G$ for all i.

Definition 1.41. *A subnormal chain is as above, though we only require that each group is normal in its predecessor.*

Definition 1.42. *A composition chain is a maximal proper subnormal chain.*

Definition 1.43. *Composition factors are the quotients of consecutive groups in a composition chain.*

Theorem 1.44. ***(Jordan-Holder)*** *The multiset of isomorphism types of composition factors is unique.*

HW 1.45. *If G is a solvable finite group and $M \overset{\min}{\lhd} G$ then M is elementary abelian.*

1.2 Permutation Groups and Actions

Definition 1.46. *A G-action on a set Ω is a homomorphism $G \longrightarrow Sym(\Omega)$ and we say that G acts on Ω*

Example 1.47. *Conjugation by a fixed group element is an action of G on itself*

DO 1.48. *Suppose G acts on Ω and there exists $g \in G$ so that $x^g = y$. In this case we say $x \sim y$. Prove that $\sim$ is an equivalence relation whose equivalence classes are orbits of G.*

DO 1.49. *(Orbit-Stabilizer) $|x^G| = |G : G_x|$*

Definition 1.50. *A G-action is transitive if it has only one orbit.*

Example 1.51. *Consider a subgroup $H \leq G$ and the coset space G/H. Define an action*

$$Ha \mapsto Hag$$

DO 1.52. *The above action is transitive; moreover these are the only transitive actions up to some equivalence (to be determined by the reader).*

HW 1.53. *If* $|\Omega| = p^k$ *for prime* p *and positive integer* k*, and* G *acts transitively on* Ω*, then* $P \in Syl_p(G) \Rightarrow P$ *is transitive.*

Consider a permutation on Ω. Observe that it has a unique cycle decomposition (product of disjoint cycles).

Definition 1.54. *The cycle type of a permutation* $\sigma \in S_n$ *is the way the lengths of the cycles partitions* n*. Example: cycle type* $(3^2, 2^5, 1^4)$ *means two 3-cycles, five 2-cycles (transpositions), and 4 fixed-points (degree* $2 \cdot 3 + 5 \cdot 2 + 4 = 20$*).*

DO 1.55. *Two permutations in* S_n *are conjugate if and only if they have the same cycle type.*