Algorithms in Finite Groups

MATH 37500: László Babai
Scribe: Angela Wu

10/14/14

5 Classification of Finite Simple Groups, Structure Theorems for Primitive Groups

5.1 Finite Simple Group Types

Theorem 5.1. All finite simple groups fall under one of the following categories

- $\mathbb{Z}_p$ for prime p.
- A_n for $n \geq 5$
- Lie type simple groups
- Sporadic groups

5.2 Lie Type simple groups

These are projective matrix groups (groups acting on projective spaces over finite fields, defined as quotients of certain matrix groups by their center, consisting of scalar matrices).
They have two subtypes: classical and exceptional groups. Each of these falls into a finite number of classes. There are 5 classes of classical groups: linear, symplectic, unitary, and three types of orthogonal groups.

5.3 Classical Lie Type – Linear

Definition 5.2. We define the projective groups $PSL(d, q)$. Let $GL(d, q)$ be the group of $d \times d$ invertible matrices over $\mathbb{F}_q$. Let $SL(d, q) := \ker(\det) \triangleleft GL(d, q)$ be the subgroup of matrices with determinant 1, where $\det : GL(d, q) \to \mathbb{F}_q$ is the determinant function. We define the projective group as the quotient of $SL(d, q)$ by its center:

$$PSL(d, q) = SL(d, q)/Z(SL(d, q)) \tag{1}$$

Exercise 5.3. $Z(SL(d, q)) = SL(d, q) \bigcap \mathbb{F}_q^\times \cdot I$

Exercise 5.4. If F is any field (finite or infinite) and $G \leq F^\times$ is finite, then G is cyclic.

Note 5.5. $|Z(SL(d,q))| = \gcd(d,q)$

5.4 Classical Lie Type – Symplectic

Definition 5.6. A symplectic bilinear form is a nondegenerate alternating bilinear form $f : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}$ satisfying (1) $f(x,y)$ is bilinear, and (2) $(\forall x \in \mathbb{F}^n)(f(x,x) = 0)$. Notice that (2) implies that $f(x,y) = -f(y,x)$ but the backwards implication is not true for fields of characteristic 2.

Definition 5.7. A symplectic space V is a vector space with a symplectic form f. We say $x \perp y$ if $f(x,y) = 0$. We define $S^\perp = \{y : (\forall s \in S)(y \perp s)\} \leq V$. We say that f is non-degenerate if its radical $\operatorname{Rad} V = 0$, where $\operatorname{Rad} V = V^\perp$.

Exercise 5.8. Show that the dimension of a nondegenerate symplectic space is even.

Theorem 5.9 (Structure Theorem)**.** If (V,f) is a nondegenerate symplectic space, then $V = V_1 \perp \ldots \perp V_k$ (orthogonal direct sum), where $\dim V_i = 2$ and $V_i = \langle v_i, w_i \rangle$ where (v_i, w_i) is a hyperbolic pair: $f(v_i, w_i) = 1$ (and therefore $f(w_i, v_i) = -1$). Generally, a symplectic space (V,f) is given by $V = \operatorname{Rad} V \perp W$ where W is a nondegenerate.

Definition 5.10. Let $Sp(V,f) := \{A : f(Ax, Ay) = f(x,y)\}$ be the group of isometries of (V,f). Let $PSp_{2n} := Sp(V,\mathbb{F})/Z(Sp(V,\mathbb{F}))$, where V has dimension $2n$.

5.5 Classical Lie Type - Orthogonal and Unitary

Exercise 5.11. Show that

1. If $char(\mathbb{F}) = p$, then $x \mapsto x^p$ is an endomorphism.
2. if $char(\mathbb{F}) = p$ and $\mathbb{F}$ is finite, then $x \mapsto x^p$ is an automorphism.
3. Show that $\operatorname{Aut}(\mathbb{F}_{p^k}) = \{x \mapsto x^{p^i} : i \ \in [k]\}$.

Exercise 5.12. Show that $\operatorname{Aut}(\mathbb{R}) = 1$. Note that $\operatorname{Aut}(\mathbb{C})$ is enormous.

something about bilinear forms and isometries (???)

Each class of classical simple groups is parametrized by a prime power (order of the field of definition) and a dimension.

5.6 Exceptional groups

Each class of exceptional simple groups is parametrized by a prime power (order of the field of definition). (The dimension is fixed in each class.)

5.7 Landazuri-Seitz

Theorem 5.13. Let G be a finite simple group of Lie type defined by its action on $PG(d-1,q)$ ($d-1$-dimensional projective space over $\mathbb{F}_q$ where $q=p^k$). Consider a nontrivial (and therefore faithful) representation $G \to GL(V)$ in *cross characteristic* (over a field of characteristic other than p). Then $\dim(V) \gtrsim q^{cd}$ for some absolute constant $c > 0$.

5.8 Structure Theorems for Primitive Groups

Theorem 5.14 (Cameron 1981)**.** Let $G \leq S_n$ be a permutation group with order $|G| > 2^{n^\epsilon}$ and n sufficiently large as a function of ϵ. Then there exist constants r, s such that

$$A_k^{(r)} \times \ldots \times A_k^{(r)} \leq G \leq S_k^{(r)} \wr S_s \tag{2}$$

where $n = \binom{k}{r}^s$ and the wreath product acts in its product action. Moreover the induced action $G \to S_s$ must be transitive.

Note that the groups described in the theorem have order $\exp(\widetilde{O}(n^{1/rs})$.
As a first step toward proving Cameron's theorem (Thm. 5.14), we make the following observations.

Exercise 5.15. Suppose that $G \leq S_n$ is primitive. We consider the minimal normal subgroups. One of the following must be hold:

1. G has at most two minimal normal subgroups. If it has two, then both of those are regular and they are each others' centralizer.

2. If G has a regular minimal normal subgroup, then, by a previous exercise, $|G| < n^{1+\log n}$. Note that this includes the case when G has an abelian minimal normal subgroup, and also the case when G has two minimal normal subgroups.

3. In the remaining cases, G has a unique minimal normal subgroup N and N is nonabelian. Therefore (N being characteristically simple) it follows that $N \cong T_1 \times \ldots \times T_k$ where $T \cong T_i$ are isomorphic nonabelian simple groups. Infer that $G \leq Aut(T) \wr S_k$.

Exercise 5.16. Show that if $G \leq S_n$ has a regular normal subgroup, then $|G| < n^{1+\log n}$. (From last time. Abelian case proved in class.)

Exercise 5.17. Suppose that $G \leq S_n$ where $|S_n : G| < 2^n$. Show that G is intransitive.