The Classical Groups

1 Introduction

'Classical' simple groups: linear groups, unitary groups, symplectic groups, orthogonal groups.

Mainly obtained by taking $G'/Z(G')$ from suitible matrix groups G.

Definition	Simplicity	Subgroups	Automorphisms & Covering groups	Isomorphisms
$PSL_n(q)$	Iwasawa's lemma	geometry	(briefly mentioned)	projective spaces

Symplectic groups: easy to understand, orders, simplicity, subgroups, covering groups, automorphisms, generic isomorphism $\mathrm{Sp}_2(q) \cong \mathrm{SL}_2(q)$, exceptional isomorphism $\mathrm{Sp}_4(2) \cong S_6$.

Unitary groups: similar to symplectic groups.

Orthogonal groups:

- fundamental differences between the cases of char$F = 2$ or odd
- subquotient is not usually simple
- to get usually simple groups, using spinor norm for odd char (see Clifford algebras and spin groups), and quasideterminant for char 2
- generic isomorphisms $\mathrm{P}\Omega_6^+(q) \cong \mathrm{PSL}_4(q)$, $\mathrm{P}\Omega_6^-(q) \cong \mathrm{PSU}_4(q)$, $\mathrm{P}\Omega_5(q) \cong \mathrm{PSp}_4(q)$ all derive from the Klein correspondence

A simple version of Aschbacher-Dynkin theorem is proved, relying heavily on representation theory.

More explicit versions for individual classes of groups see Kleidman and Liebeck's book.

Some exceptional behavior of small classical groups is related to exceptional Weyl groups.

2 Finite fields

Please refer to literatures about finite fields for more details.

Definition 2.1. *field* $(F, +, \cdot)$

Lemma 2.2. *All non-zero elements have the same additional order of prime p.*

Proof. $F^\times \curvearrowright F^+ \backslash \{0\}$ by multiplication as group automorphism (distributive law) transitively. □

Definition 2.3. *The p above is the **characteristic** of F. $F_0 := \langle 1 \rangle_+$ is the **prime subfield** of F.*

Lemma 2.4. $|F| = p^d$

Proof. F is a vector space over F_0. □

Lemma 2.5. $F^\times = \langle \sigma \rangle \cong \mathbb{Z}_{p^d-1}$*, where σ is called a **Singer cycle**.*

Proof. By Vandermonde's lemma, polynomial of degree n on F has at most n solutions in F. $e := \exp(F^\times) < |F^\times| \implies x^e - 1 = 0$ has $|F^\times| > e$ solutions. $\square$

Proposition 2.6. *For any prime power $q = p^d$, $\exists_1 F$ of order q up to field isomorphism, says $\mathbb{F}_q$.*

Proof. Existance: $\mathbb{Z}/p\mathbb{Z}[x]/(f(x))$ for any irreducible polynomial $f(x)$ of degree d.

Uniqueness: If $|F| = p^d$, then $F_0 \cong \mathbb{F}_p$, F is the splitting field of $x^{p^d} - x$ over F_0, $F^\times = \langle x \rangle$. $\square$

Lemma 2.7. $\mathrm{Aut}(\mathbb{F}_q) = \langle \phi \rangle \cong \mathbb{Z}_d$, *where $\phi : x \mapsto x^p$ is called the* ***Frobenius automorphism****.*

3 General linear groups

Lemma 3.1 (Iwasawa)**.** *If finite group G satisfies the following conditions, then G is simple.*

i. $G' = G$*;*

ii. *G is primitive on some set Ω;*

iii. *$\exists A \trianglelefteq G_\alpha$ such that A is solvable;*

iv. $G = A^G$*.*

i.e. A perfect primitive group G, being the normal closure of an abelian normal subgroup A of its point stabilizer, is simple.

Proof. Suppose that $1 \neq N \trianglelefteq G$. Then, by primitivity, N is transitive on Ω and hence $G = G_\alpha N$. For any $g \in G$, $g = hn$ for some $h \in G_\alpha$ and $n \in N$.

Then $a^g = a^{hn} = a^n$, $\forall a \in A$, since $A \trianglelefteq G_\alpha$. Moreover, $a^n = a(n^{-1})^a n \in AN$ since $N \trianglelefteq G$. Thus $G = A^G = AN$.

Now, $G/N = AN/N = A/(A \cap N)$ is solvable. Meanwhile, $(G/N)' = G'N/N = GN/N = G/N$. Thus $G/N = 1$ and $G = N$, G is simple. $\square$