19 Automorphisms (11/06)

19.1 ϵ more on matrix groups

There are many other types of matrix groups one can cook up.

Example 19.1 (Upper-triangular matrices)**.** Let $\mathbf{B}_n(k) \subseteq \mathbf{GL}_n(k)$ be the subgroup of invertible upper-triangular matrices. The order of $\mathbf{B}_2(\mathbf{F}_p)$ is $p(p-1)^2$. There is also the group of special upper-triangular matrices, i.e., the subgroup of $\mathbf{SB}_n(k)$ of elements with determinant 1. The order of $\mathbf{SB}_2(\mathbf{F}_p)$ is $p(p-1)$.

Example 19.2 (Unipotent matrices)**.** Let $\mathbf{U}_n(k) \subseteq \mathbf{GL}_n(k)$ be the subgroup of upper-triangular matrices with 1s on the diagonal. The order of $\mathbf{U}_2(\mathbf{F}_p)$ is p. The order of $\mathbf{U}_3(\mathbf{F}_p)$ is p^3.

19.2 The dream of finite groups

We now have at our disposal the powerful Sylow theorems to help us understand finite groups. With them, we can prove the existence of large p-groups inside a given group, if p divides the order, and in some situations these large p-groups are normal. In addition, the structure of p-groups seems to be somewhat tractable as the center of a non-trivial p-group is always non-trivial.

Understanding finite groups and their classification now boils down to two main problems,

(a) to understand the finite simple groups, i.e., those with no non-trivial normal subgroups, and

(b) to understand how to build every group out of simple groups;

together with these I will add the problem

(c) of understanding the p-groups and hence all possible p-Sylow subgroups.

We will not complete this task in this course and in fact the task is as of yet incomplete for humanity as a whole. However, in the 1980s, mathematicians did complete task (a), the classification of all finite simple groups. There are infinitely many (such as the $\mathbf{Z}/p$ for primes p), but they sit inside certain specific families except for finitely many exceptions.

19.3 Automorphisms

In general, it is difficult to say how a group is "built up out of" its subgroups. But, there is one important exception that we will discuss this week, namely the semidirect products. To understand these, we first have to say a little bit about automorphisms of groups.

Definition 19.3 (Automorphisms)**.** Given a group G, and **automorphism** of G is bijective group homomorphism (or, group isomorphism) $f\colon G \to G$.

Definition 19.4. Give a group G, we write $\mathrm{Aut}(G)$ for the group of automorphisms of G. That is,

$$\mathrm{Aut}(G) = \{f\colon G \to G \mid f \text{ is a group isomorphism}\}.$$

This is a group under composition.

Remark 19.5. We can view $\mathrm{Aut}(G)$ as sitting inside S_G. Whereas S_G consists of all permutations of G, or all functions $f\colon G \to G$, the group $\mathrm{Aut}(G)$ consists of only those permutations that behave well with respect to the group structure on G.

Example 19.6. The group $\mathrm{Aut}(\mathbf{Z})$ is isomorphic to $\{\pm 1\} \cong \mathbf{Z}/2$. Indeed, a group homomorphism $f\colon \mathbf{Z} \to \mathbf{Z}$ is determined by where it sends 1. It is a group isomorphism if and only if it sends 1 to 1 or -1 in $\mathbf{Z}$.

Example 19.7. The only automorphism of $\mathbf{Z}/2$ is the identity. Thus, $\mathrm{Aut}(\mathbf{Z}/2) = \{\mathrm{id}_{\mathbf{Z}/2}\}$ is the trivial group.

Example 19.8. An automorphism of $\mathbf{Z}/3$ can send 1 to 1 or to 2. Thus, $\mathrm{Aut}(\mathbf{Z}/3) \cong \mathbf{Z}/2$.

Example 19.9. An automorphism of $\mathbf{Z}/4$ can send 1 to either 1 or 3. Again, $\mathrm{Aut}(\mathbf{Z}/4) \cong \mathbf{Z}/2$.

19.4 Exercises

Exercise 19.1. Determine the number of p-Sylow subgroups in $\mathbf{B}_2(\mathbf{F}_p)$.

Exercise 19.2. Compute the order of $\mathbf{GL}_n(\mathbf{F}_p)$ following the idea of Example 18.9.

Exercise 19.3. Justify the claim in Example 19.6. Specifically, show that if $f\colon \mathbf{Z} \to \mathbf{Z}$ is an automorphism, then $f(1) = 1$ or -1.

Exercise 19.4. Compute the order of $\mathrm{Aut}(\mathbf{Z}/n)$ for all $n \geqslant 2$.