Homework Assignment 7

Due Friday, March 13

There are two parts to this homework. The first part outlines a proof of the Jordan-Hölder theorem, while the second introduces a new class of examples of finite groups.

1 Jordan-Hölder

Recall the following defintion from class.

Definition 1. *Let G be a group. A sequence of subgroups:*

$$1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_k = G,$$

is called a composition series if for each i $N_i \trianglelefteq N_{i+1}$ and the quotient N_{i+1}/N_i is normal.

The important point is that composition series exist, and are in some sense unique.

Theorem 1 (Jordan-Hölder)**.** *Let G be a finite group with $G \neq 1$. Then,*

(1) G has a composition series.

(2) The composition factors of the composition series are unique. Specifically, this means that if

$$1 = N_0 \leq N_1 \leq \cdots \leq N_k = G,$$

$$1 = M_0 \leq M_1 \leq \cdots \leq M_s = G,$$

are two composition series', then $s = k$ and there is a permutation π of $\{1, \cdots, k\}$ such that

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1},$$

for each i.

1. This first exercise proves the Jordan-Hölder theorem.
   (a) Prove part (1) of the Jordan-Hölder theorem by induction on $|G|$.
   (b) Prove part (2) if the Jordan-Hölder theorem in the case that $s = 2$. (Hint: Show if H,K are normal subgroups, then so is HK, then use the second isomorphism theorem with M_1 and N_{k-1}).
   (c) Prove part (2) of the Jordan-Hölder theorem by induction on the minimum of r and s. (Apply the inductive hypothesis to $H = N_{r-1} \cap M_{s-1}$).

2 Matrix Groups

The rest of the homework introduces a new family of finite groups. So far we've only studies a few examples of finite groups: D_{2n}, S_n and direct products of cyclic groups. As we start defining more exotic properties of groups we will need to expand our library of finite groups to exhibit some of these interesting properties. In this homework we will introduce a new example: finite matrix groups. We will need a definition.

Definition 2. *A field is a set F together with two commutative binary operations, $+$ and $\cdot$ (addition and multiplication), such that $(F, +)$ and $(F\backslash\{0\}, \cdot)$ are abelian groups, and such that the distributive law holds. That is, for all $a, b, c \in F$ we have:*

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

For any field we let $F^\times = F \setminus \{0\}$ be its mutliplicative group. A field F is called a finite field if $|F| < \infty$.

It turns out that vector space theory over F is pretty much identical to vector space theory over R. We can define the first matrix group we hope to study.

Definition 3. *Let F be a field. If M, N are matrices with entries in F, we can compute their product MN and the determinant $\det(M) \in F$ using the same formulas as if $F = \mathbb{R}$. Then the general linear group of degree n over F is,*

$$GL_n(F) = \{A \mid A \textit{ is an } n \times n \textit{ matrix with entries in } F \textit{ and } \det(A) \neq 0\}.$$

2. It turns out that we have seen exampless of finite fields already.
   (a) Let p be a prime number. Show that $\mathbb{Z}/p\mathbb{Z}$ with the operations $+$ and $\times$ is a field. This is the *finite field of order p* and will be denoted by $\mathbb{F}_p$.
   (b) Show that if n is not prime, $\mathbb{Z}/n\mathbb{Z}$ is not a field.

3. Let's study the simplest example of general linear groups: $GL_2(F)$.
   (a) Let $A, B \in GL_2(F)$. Show that $\det(AB) = \det(A)\det(B)$.
   (b) Show that $\det(A) = 0$ if and only if one row is a multiple of the other.
   (c) Show that $A^{-1} = \frac{1}{\det(A)}\tilde{A}$ where $\tilde{A}$ is defined by the rule:
   $$\widetilde{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$
   (d) Conclude that $GL_2(F)$ is a group, and that $\det : GL_2(F) \to F^\times$ is a homomorphism.
   (e) Prove that $GL_2(F)$ is isomorphic to the group G of linear ismorphisms from $F^2 \to F^2$. (Hint, use matrix multiplication to get a map $GL_2(F) \to G$.)

   As you may have noticed, this proof went through the same way it does for $F = \mathbb{R}$ in linear algebra. The proofs can get more computationally intense for $GL_n(F)$ as n increases, so for now lets take on faith that $GL_n(F)$ is a group and $\det : GL_n(F) \to F^\times$ is a homomorphism, and that $GL_n(F)$ parametrizes linear automorphisms of F^n.

4. Now let's study $GL_2(\mathbb{F}_p)$.
   (a) Prove that $|GL_2(\mathbb{F}_2)| = 6$.
   (b) Write all the elements of $GL_2(\mathbb{F}_2)$ and compute the order of each element.
   (c) Show that $GL_2(\mathbb{F}_2)$ is not abelian. (We will later see that it is isomorphic to S_3).
   (d) Generalizing part (a), show that if p is prime then
   $$|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p.$$
   Use exercise 3(b).

5. The general linear group has lots of interesting subgroups and quotients.

   (a) Show that the constant diagonal matrices are a normal subgroup of $GL_n(F)$ isomorphic to $F^\times$

   We will often abuse notation and denote this by $F^\times \trianglelefteq GL_n(F)$. The quotient group $GL_n(F)/F^\times$ is called the *projective general linear group* and denoted $PGL_n(F)$.

   (b) The *special linear group* $SL_n(F)$ is defined

   $$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1.\}$$

   Show that $SL_n(F)$ is a normal subgroup of $GL_n(F)$.

   (c) Prove the following isomorphism.

   $$GL_n(F)/SL_n(F) \cong F^\times.$$

   (d) List all the elements of $SL_2(\mathbb{F}_2)$

   (e) Use problem 3(d) to compute $|SL_2(\mathbb{F}_p)|$.

   (f) Let I be the identity matrix. Show that $\{\pm I\} \leq SL_n(F)$ if and only if n is even.

   (g) Use the second isomorphism theorem to construct an isomorphism:

   $$PGL_2(F) \cong SL_2(F)/\{\pm I\}.$$