12/1/15

HW 4 due this Thurs.
Please note that I fixed a typo in the hints to Problem 2(c).

The Final Exam is next Thurs Dec 10 at 2:00 - 4:30 pm. We will have a review session next Tuesday in class.

---

This Week: Epilogue.

Recall the Sylow Theorems: Let $G$ be a finite group and let $p \in \mathbb{Z}$ be prime. Suppose that $|G| = p^a m$ with $p \nmid m$.

(1) There exists a subgroup $P \subseteq G$ with size $|P| = p^a$.

(2) Given subgroups $P, Q \subseteq G$ with $|P| = p^\alpha$ and $|Q| = p^\beta$ ($\beta \leq a$), there exists a group element $g \in G$ such that

$$gQg^{-1} \subseteq P.$$

(3) If $n_p = \#\{P \subseteq G : |P| = p^\alpha\}$ then we have

- $n_p \equiv 1 \bmod p$
- $n_p \mid m$ //

We saw last time that these results are a powerful tool for studying the structure of finite groups. Let me summarize some results.

- If $|G| = p^\alpha$ then $G$ is solvable with composition length $\alpha$. It is simple if and only if $\alpha = 1$.

- Let $|G| = pq$ with $p < q$ prime. If $p \nmid (q-1)$ then $G$ is cyclic. If $p \mid (q-1)$ then $G$ is either cyclic or

$$G \approx \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x, y \in \mathbb{Z}_q\mathbb{Z},\ x^p = 1 \right\},$$

which is non-abelian.

- If $|G| = pqr$ with $p < q < r$ prime then $G$ is not simple. More generally, if $|G| = p_1 p_2 \cdots p_k$ with $p_1 < p_2 < \cdots < p_k$ prime, then $G$ is solvable. [You can prove this by induction.]

- Let $|G| = p^r m$ with $p \nmid m$. If $m$ has no divisor $d \mid m$ with $d \neq 1$ and $d = 1 \bmod p$ then $G$ is not simple.

- Burnside's Theorem (1904):

  If $|G| = p^r q^s$ with $p < q$ prime then $G$ is solvable.

  [The proof uses representation theory and is beyond the scope of the course.]

- Feit-Thompson Theorem (1962):

  If $|G|$ is odd then $G$ is solvable.

  [The proof is ~250 pages and is way beyond the scope of the course.]

//

We thus have a lot of restrictions on the possible sizes of finite simple groups.

↓

Apart from the abelian simple groups (i.e., $\mathbb{Z}/p\mathbb{Z}$ for prime $p$), the smallest possible size of a simple group is

$$60 = 2^2 \cdot 3 \cdot 5.$$

We know that such a simple group *does* exist, and its existence is the reason that polynomial equations of degree $\geq 5$ are not solvable by radicals.

This suggests that finite simple groups might have important connections to other parts of mathematics, and indeed they do.

Let me list some of the smallest simple groups. Recall that $A_n$ is the alternating subgroup of $S_n$ defined by

$$1 \longrightarrow A_n \longrightarrow S_n \xrightarrow{\det} \mathbb{Z}^\times \longrightarrow 1$$

and $PSL_n(q) := SL_n(\mathbb{F}_q) / Z(SL_n(\mathbb{F}_q))$, where $q = p^k$ with $p$ prime, $\mathbb{F}_q$ is the field of size $q$, and

↓

$SL_n(\mathbb{F}_q)$ is the special linear group defined by

$$1 \longrightarrow SL_n(\mathbb{F}_q) \longrightarrow GL_n(\mathbb{F}_q) \xrightarrow{\det} \mathbb{F}_q^{\times} \longrightarrow 1 .$$

These definitions give us all of the simple groups up to size 6000 :

| $\lvert G \rvert$ | simple group $G$ |
|---|---|
| 60 | $A_5 = PSL_2(4) = PSL_2(5)$ |
| 168 | $PSL_2(7) = PSL_3(2)$ |
| 360 | $A_6 = PSL_2(9)$ |
| 504 | $PSL_2(8)$ |
| 660 | $PSL_2(11)$ |
| 1092 | $PSL_2(13)$ |
| 2448 | $PSL_2(17)$ |
| 2520 | $A_7$ |
| ⋮ | ⋮ |

There are other families of finite simple groups coming from the simple lie algebras. For example, if $q$ is a prime power then there exists a family of simple groups $E_8(q)$ with sizes

$$|E_8(q)| = q^{120} \prod_{i \in I} (q^i - 1)$$

where $I = \{2, 8, 12, 14, 18, 20, 24, 30\}$.

And then there are 26 sporadic simple groups that are not part of infinite families. The largest of these is called the monster $\mathbb{M}$. It has size

$$|\mathbb{M}| \approx 8 \cdot 10^{53}.$$

It seems that there is a huge amount of mathematics hidden inside these groups. For example, Borcherds won the Fields medal in 1992 for proving the "monstrous moonshine" conjecture relating $\mathbb{M}$ to the mathematics of string theory and modular forms.

We know that

$$|A_n| = |S_n|/2$$

$$= n!/2$$

$$= 3 \cdot 4 \cdot 5 \cdots (n-1) \cdot n$$

and I mentioned previously that

$$|PSL_n(q)| = \frac{q^{\binom{n}{2}}(q^2-1)(q^3-1)\cdots(q^n-1)}{\gcd(n, q-1)}$$

but I never proved this. Let me prove it now, since it is relevant to HW6 Problem 4.

★ Theorem:

$$|GL_n(q)| = q^{\binom{n}{2}}(q-1)(q^2-1)\cdots(q^n-1).$$

Proof: The columns of an invertible $n \times n$ matrix over $\mathbb{F}_q$ form an ordered basis of the vector space $(\mathbb{F}_q)^n$,

and it is not difficult to count these.

To create an ordered basis $b_1, b_2, \dots, b_n \in \mathbb{F}_q^n$,

first choose $b_1 \in \mathbb{F}_q^n - 0$ in $q^n - 1$ ways

then choose $b_2 \in \mathbb{F}_q^n - \langle b_1 \rangle$ in $q^n - q^1$ ways

then choose $b_3 \in \mathbb{F}_q^n - \langle b_1, b_2 \rangle$ in $q^n - q^2$ ways.

Continuing in this way gives

$$|GL_n(q)| = (q^n-1)(q^n-q^1)(q^n-q^2)\cdots(q^n-q^{n-1})$$

$$= (q^n-1)\,q\,(q^{n-1}-1)\,q^2\,(q^{n-2}-1)\cdots q^{n-1}(q^1-1)$$

$$= q^{1+2+\cdots+(n-1)}(q-1)(q^2-1)\cdots(q^n-1)$$

$$= q^{\frac{n(n-1)}{2}}(q-1)(q^2-1)\cdots(q^n-1)$$

$$= q^{\binom{n}{2}}(q-1)(q^2-1)\cdots(q^n-1),$$

as desired.

[Remark: There is alternative notation for this that emphasizes the analogy between $S_n$ and $GL_n$. For all $m \in \mathbb{N}$ we define

$$[m]_q := 1 + q + q^2 + \cdots + q^{m-1} = \frac{q^m - 1}{q - 1}.$$

Note that $[m]_q \to m$ as $q \to 1$. We call this a "$q$-analogue" or a "quantum analogue" of the integer $m$. Then for $n \in \mathbb{N}$ we define the $q$-factorial

$$[n]_q! := [1]_q [2]_q \cdots [n-1]_q [n]_q.$$

$$= \frac{q-1}{q-1} \cdot \frac{q^2-1}{q-1} \cdots \frac{q^{n-1}-1}{q-1} \cdot \frac{q^n-1}{q-1}.$$

Now we can easily see that

$$|GL_n(q)| = q^{\binom{n}{2}} (q-1)^n [n]_q! \quad ]$$

✡ Corollary:

$$|SL_n(q)| = q^{\binom{n}{2}} (q^2-1)(q^3-1)\cdots(q^n-1).$$

Proof: Since the sequence

$$1 \to SL_n(q) \to GL_n(q) \to \mathbb{F}_q^{\times} \to 1$$

is exact we have

$$|SL_n(q)| = |GL_n(q)| \,/\, |\mathbb{F}_q^{\times}|$$

$$= |GL_n(q)| \,/\, (q-1). \qquad ///$$

Next, we need to compute the size of the center $Z(SL_n(q))$. Here is a general fact.

✡ Theorem: Let $K$ be a field. Then we have

$$Z(GL_n(K)) = \{ \alpha I : \alpha \in K^{\times} \}$$

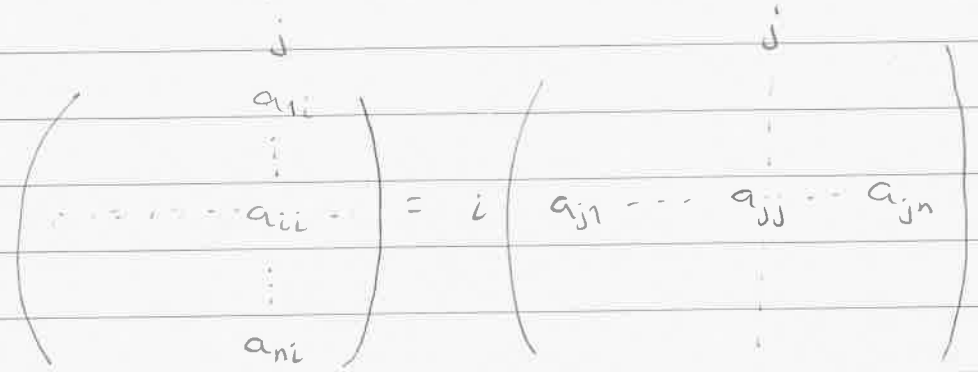
$$Z(SL_n(K)) = \{ \alpha I : \alpha \in K^{\times}, \alpha^n = 1 \}.$$

Proof: Suppose that $A = (a_{ij}) \in Z(GL_n(K))$. Let $e_{ij}(\alpha)$ be the matrix with $(i,j)$ entry $\alpha$ and zeroes elsewhere, and define the elementary matrix

$$E_{ij}(\alpha) := I + e_{ij}(\alpha).$$

For $i \neq j$ note that $E_{ij}(\alpha)$ is invertible with $\det(E_{ij}(\alpha)) = 1$, hence $E_{ij}(\alpha) \in SL_n(K)$.

Since $A$ commutes with $E_{ij}(1)$ it must also commute with $e_{ij}(1)$. Then the equation $Ae_{ij}(1) = e_{ij}(1)A$ says




which implies that $a_{ij} = 0$ and $a_{ii} = a_{jj}$ for all $i \neq j$. We conclude that

$$A = \alpha I \quad \text{for some } \alpha \in K^\times.$$

If $A \in SL_n(K)$ we must also have

$$\alpha^n = \det(\alpha I) = 1.$$

///

Remark: This proof works more generally when $K$ is a commutative ring with 1.

Finally, we need to count the $n^{th}$ roots of unity in the field $\mathbb{F}_q$.

✡ Theorem:

$$|Z(SL_n(q))| = gcd(n, q-1)$$

Proof: By the previous theorem we have

$$|Z(SL_n(q))| = \#\{\alpha \in \mathbb{F}_q^\times : \alpha^n = 1\}.$$

Recall that the primitive root theorem says that $\mathbb{F}_q^\times = \langle g \rangle$ is cyclic of order $q-1$.

Thus we want to count integers $x \in \mathbb{Z}$ such that $0 \leq x < q-1$ and $(g^x)^n = 1$. Note that

$$(g^x)^n = 1 \iff g^{xn} = 1 \iff xn = 0 \pmod{q-1}$$

To find such $x$ we will solve the linear Diophantine equation

$$(*) \qquad xn + y(q-1) = 0$$

for $x, y \in \mathbb{Z}$. The equation translates to

$$-\frac{x}{y} = \frac{q-1}{n}$$

If $d = \gcd(n, q-1)$ then the most general way to write this fraction is

$$-\frac{x}{y} = \frac{k(q-1)/d}{kn/d}$$

and it follows that the general solution of ⊛ is

$$(x, y) = \left(k\frac{q-1}{d}, -k\frac{n}{d}\right), \quad k \in \mathbb{Z}.$$

After reducing mod $q-1$ we find that the general solution of $xn \equiv 0 \pmod{q-1}$ is given by

$$x \equiv \frac{k(q-1)}{d} \pmod{q-1}.$$

and there are $d$ distinct solutions:

$$x = 0, \frac{q-1}{d}, 2\cdot\frac{q-1}{d}, \ldots, (d-1)\cdot\frac{q-1}{d}.$$

12/3/15

HW4 extended until Tues.
Review session Tues.
Final Exam next Thurs 2:00 - 4:30pm

Today: Epilogue Part 2.

Last time I discussed the classification of finite simple groups. To classify all finite groups we would need to describe all the ways to put groups together (the "extension problem") but this turns out to be extremely complicated.

Example: If $|G| = p^k$ where $p$ is prime then we know that the composition factors of $G$ are just

$$\underbrace{\mathbb{Z}/p, \mathbb{Z}/p, \mathbb{Z}/p, \cdots, \mathbb{Z}/p}_{k \text{ times.}}$$

However, there are a ridiculous number of ways to put the composition factors together.

Specifically, Higman proved in 1960 that the number of groups of size $p^k$ is

$$\geq p^{\frac{2}{27}k^2(k-6)}.$$

For example, the number of groups of size $1024 = 2^{10}$ is

$$49,487,365,422. \quad ///$$

[Remark: In fact, over 99% of the groups of size $\leq 2000$ have size 1024.]

No one really expects to "solve" the problem of p-groups, and since every finite group is built out of its Sylow p-subgroups, no one really expects to "solve" the problem of finite groups.

However, the problem of finite <u>abelian</u> groups is much easier. For example, there are only 42 abelian groups of size 1024. We'll prove this next semester; today I'll just state the theorem and discuss some applications.

Let $G$ be an abelian group of size

$$|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1, p_2, \ldots, p_k$ are distinct primes. For each $i$ let $P_i \subseteq G$ be a subgroup of size $|P_i| = p_i^{\alpha_i}$, i.e., a Sylow $p_i$-subgroup.

Since $G$ is abelian each $P_i \subseteq G$ is normal. Since the sizes of the $P_i$ are coprime we obtain a direct product decomposition

$$(*) \qquad G = P_1 \times P_2 \times \cdots \times P_k .$$

Furthermore, this expression is unique since each normal Sylow subgroup is unique. We call $(*)$ the primary decomposition of $G$.

Thus to understand the structure of finite abelian groups we only need to investigate the structure of abelian $p$-groups. The answer turns out to be remarkably simple:

## ☆ Fundamental Theorem of Finite Abelian Groups:

Every abelian p-group is a direct product of cyclic groups, hence the same is true of any finite abelian group. ///

However, the F.T.F.A.G. is not easy to prove with our current technology. [I tried to present the proof from Aluffi page 236-237 but it was too complicated for my taste and it resulted in a bad lecture :(. ] The correct proof is based on a completely new point of view: thinking of a finite abelian group as a "finite-dimensional vector space over $\mathbb{Z}$" and then using the machinery of Gaussian elimination. We will develop this point of view in the spring and it will allow us to see that the F.T.F.A.G. is really the "same thing" as the Jordan Canonical Form of a matrix.

For now let's see some examples and a fun application.

Example: The abelian groups of size $32 = 2^5$ are

- $\mathbb{Z}/(2^5)$
- $\mathbb{Z}/(2^4) \times \mathbb{Z}/(2^1)$
- $\mathbb{Z}/(2^3) \times \mathbb{Z}/(2^2)$
- $\mathbb{Z}/(2^3) \times \mathbb{Z}/(2^1) \times \mathbb{Z}/(2^1)$
- $\mathbb{Z}/(2^2) \times \mathbb{Z}/(2^2) \times \mathbb{Z}/(2^1)$
- $\mathbb{Z}/(2^2) \times \mathbb{Z}/(2^1) \times \mathbb{Z}/(2^1) \times \mathbb{Z}/(2^1)$
- $\mathbb{Z}/(2^1) \times \mathbb{Z}/(2^1) \times \mathbb{Z}/(2^1) \times \mathbb{Z}/(2^1) \times \mathbb{Z}/(2^1)$.

Note that these are in bijection with partitions of the integer 5:

- 5
- 4+1
- 3+2
- 3+1+1
- 2+2+1
- 2+1+1+1
- 1+1+1+1+1.

For any prime $p$, the abelian groups of size $p^k$ are in bijection with integer partitions of $k$. Recall that the number of these is given by the Hardy-Ramanujan asymptotic formula ↓

$$\frac{1}{4k\sqrt{3}} \exp\left(\pi\sqrt{\frac{2k}{3}}\right),$$

which is big, but still <u>much</u> smaller than Higman's bound. ///

Example: Consider the following random abelian group of size $360 = 2^3 \cdot 3^2 \cdot 5^1$:

$$G = \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(5)$$

Is there a more efficient way to describe this group? Yes. To see this we first recall the following lemma.

☆ Lemma: Given $a, b \in \mathbb{Z}$ with $\gcd(a,b) = 1$ we have

$$\mathbb{Z}/(a) \times \mathbb{Z}/(b) \cong \mathbb{Z}/(ab).$$

Proof: Let $\mathbb{Z}/(a) = \langle x \rangle$ and $\mathbb{Z}/(b) = \langle y \rangle$ Then the element $(x,y) \in \langle x \rangle \times \langle y \rangle$ has order

}

$$|\langle (x,y) \rangle| = \text{lcm}(|\langle x \rangle|, |\langle y \rangle|)$$
$$= \text{lcm}(a,b)$$
$$= a \cdot b / \gcd(a,b)$$
$$= a \cdot b$$

and hence

$$\mathbb{Z}/(a) \times \mathbb{Z}/(b) = \langle (x,y) \rangle$$

is cyclic. ///.

There are several ways to apply this to our group $G$ but one is more efficient than all the others:

$$G = (\mathbb{Z}/(2)) \times (\mathbb{Z}/(2) \times \mathbb{Z}/(3)) \times (\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(5))$$

$$\approx \mathbb{Z}/(2) \times \mathbb{Z}/(6) \times \mathbb{Z}/(30).$$

This most efficient encoding is characterized by the fact that

$$2 \mid 6 \mid 30.$$

These three numbers are called the "invariant factors" of $G$. ///

In general, given a finite abelian group $G$ there exist unique integers $2 \leq d_1, d_2, \cdots, d_m$ (called the invariant factors of $G$) such that

- $d_1 \mid d_2 \mid \cdots \mid d_m$
- $|G| = d_1 d_2 \cdots d_m$
- $G \approx \mathbb{Z}/(d_1) \times \mathbb{Z}/(d_2) \times \cdots \times \mathbb{Z}/(d_m)$. ///

The proof is algorithmic, so let's just do an example.

Example: Find the invariant factors of

$$G = \prod_{i,j} \frac{\mathbb{Z}}{p_i^{\alpha_{ij}}\mathbb{Z}}$$

when $\{p_i^{\alpha_{ij}}\} = \{2^1, 2^3, 3^1, 3^1, 3^4, 5^1, 5^1, 7^2\}$.

To do this we arrange the numbers $p_i^{\alpha_{ij}}$ (called the elementary divisors of $G$) in a table so that exponents decrease along columns:

$$2^3\ 3^4\ 5^1\ 7^2 \rightarrow 158760$$
$$2^1\ 3^1\ 5^1 \rightarrow 30$$
$$3^1 \rightarrow 3$$

The invariant factors are given by the products of the rows:

$$3 \mid 30 \mid 158760$$

The F.T.F.A.G. is quite useful because it gives us shortcuts to lots of theorems about abelian groups. Here is one striking example.

☆ Lemma: Let $G$ be a finite abelian group and assume that for all integers $n \geq 0$ the number of elements $g \in G$ such that $g^n = 1$ is at most $n$. Then $G$ is cyclic.

Proof: Suppose $G$ has invariant factors

$$d_1 \mid d_2 \mid \cdots \mid d_m .$$

and assume for contradiction that $m \geq 2$.

Then since $|G| = d_1 d_2 \cdots d_m$ and $2 \leq d_1, \ldots, d_m$ we have $d_m < |G|$. Furthermore, since

$$G \simeq \mathbb{Z}/(d_1) \times \mathbb{Z}/(d_2) \times \cdots \times \mathbb{Z}/(d_m)$$

and $d_1 | d_2 | \cdots | d_m$ we have $g^{d_m} = 1$ for all $g \in G$. We have found an integer $n = d_m$ such that there exist more than $n$ elements $g \in G$ with $g^n = 1$.

//

★ Primitive Root Theorem:

Let $K$ be a field. Then any finite subgroup of $K^\times$ is cyclic. In particular, if $K$ is finite then $K^\times$ is cyclic.

Proof: Let $n$ be a non-negative integer and consider the polynomial $x^n - 1 \in K[x]$. Now recall from your previous life that a polynomial of degree $n$ over a field has at most $n$ roots. This completes the proof.

//

That was cute right? I like this proof much better than messing around with the Euler totient function and I think it illustrates the power of the F.T.F.A.G. //

Remark: The theory of abelian groups is really very different from the theory of general groups. It is more rightly seen as an aspect of the theory of modules, which will be our main topic in MTH 762.

See you then!