Math 128A, Mon Nov 09

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: Ch. 11. Reading for one week from today: Ch. 12. Rings!
- PS09 outline due today, full version due in 1 week.
- **NO CLASSES ON WED NOV 11 — VETERANS DAY**
- Problem session, Fri Nov 13, 10:00–noon on Zoom. PS08 PS09

Exam 3 in 2wks

The Fundamental Theorem of Finite Abelian Groups

Theorem

Let G be a finite abelian group.

1. *G is isomorphic to an external direct product of cyclic groups of prime power order:*

$$G \approx \mathbf{Z}_{p_1^{n_1}} \oplus \mathbf{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbf{Z}_{p_k^{n_k}}$$

2. *This product is unique, assuming that (a) $p_1 \leq p_2 \leq \cdots \leq p_k$ and (b) if $p_i = p_{i+1}$, then $n_i \leq n_{i+1}$. (I.e., parts corresponding to each prime appear in increasing order by prime, and prime powers appear in increasing order by prime.)*

Note that as a consquence, two finite abelian groups with different decompositions into external direct products of cyclic groups of prime power order cannot be isomorphic.

e.g. $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{16} \not\approx \mathbb{Z}_4 \oplus \mathbb{Z}_{\varepsilon} \oplus \mathbb{Z}_4$

Example: Classify finite abelian groups of order $7^3 11^4$

First: To see the different ways to express 11^4 as a product of powers of 11, we use partitions; that is:

$4 = 4$	11^4
$= 3+1$	$11^3 \cdot 11^1$
$= 2+2$	$11^2 \cdot 11^2$
$= 2+1+1$	$11^2 \cdot 11 \cdot 11$
$= 1+1+1+1$	$11 \cdot 11 \cdot 11 \cdot 11$

Abgps of order 11^4

$\mathbb{Z}_{11^4}$, $\mathbb{Z}_{11^3} \oplus \mathbb{Z}_{11}$, $\mathbb{Z}_{11^2} \oplus \mathbb{Z}_{11^2}$, $\mathbb{Z}_{11^2} \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11}$, $\mathbb{Z}_{11} \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11}$

$\mathbb{Z}_{7^3}$ 3

$\mathbb{Z}_{7^2} \oplus \mathbb{Z}_7$ 2+1

$\mathbb{Z}_7 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$ 1+1+1

Partitions of 3

$\mathbb{Z}_{11^4}$

$\mathbb{Z}_{11^3} \oplus \mathbb{Z}_{11}$

$\mathbb{Z}_{11^2} \oplus \mathbb{Z}_{11^2}$

$\mathbb{Z}_{11^2} \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11}$

$\mathbb{Z}_{11} \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11}$

Every ab group of order 11^4 is isomorphic to exactly one group on this list and no others.

That means that there are 15 finite abelian groups of order 7^3*11^4, up to isomorphism, and they are obtained like ordering takeout from a restaurant: one from Column A, one from Column B, and so on.

Ex.

$\mathbb{Z}_{7^2} \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{11^2} \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11}$

$\mathbb{Z}_{7^3} \oplus \mathbb{Z}_{11^3} \oplus \mathbb{Z}_{11}$

(13 others) If $|G| = 7^3 11^4$

$\mathbb{Z}_{49} \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{121} \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11} = G$

or $G = \mathbb{Z}_{343} \oplus \mathbb{Z}_{1331} \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11}$ ← not $\approx$

Q: If we encounter a finite abelian group G "in the wild" (i.e., we come across a finite abelian group that we don't already understand as an external direct product of cyclic groups), how can we figure out which product of cyclic groups of prime power order G is isomorphic to?

A: One method: Look at orders of elements in G. (Brute force, but brute force with a plan, at least.)

Example: A subgroup of $U(200)$

$|G| = 16$

Consider

-1

$$G = \{1, 7, 43, 49, 51, 57, 93, 99, 101, 107, 143, 149, 151, 157, 193, 199\},$$

4 4 2 2 4 4 2 2 4 4 2 2 4 4 2

with operation multiplication (mod 200), i.e., consider G as a subgroup of $U(200)$.

Since G is a finite abelian group, G is isomorphic to an external direct product of cyclic groups of prime power order. Which one?

Ans: First list all abelian groups of order $|G| = 16 = 2^4.$

4	$\mathbb{Z}_{16}$
3+1	$\mathbb{Z}_8 \oplus \mathbb{Z}_2$
2+2	$\mathbb{Z}_4 \oplus \mathbb{Z}_4$
2+1+1	$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
1+1+1+1	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Order of 7 in G by brute force

$7^1=7$, $7^2=49$, $7^3=343=143$

$\;\| \\ (50-1)$ $\quad 7^4=2500-100+1=1$ (mod 200)

$\mathrm{ord}(7)=4 \quad \mathrm{ord}(49)=2, \; \mathrm{ord}(143)=4$

$51^2=2601=1 \qquad 101^2=10201=1$

$193=-7$; $(-7)^2=49$; $(-7)^3=57$, $(-7)^4=1$

$107^2=11449=49 \qquad 107^3=107\cdot 49$

$$= \begin{array}{r} 4900 \\ 343 \end{array} = 43$$

So: Largest order is 4. $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ or $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$\mathbb{Z}_4 \oplus \mathbb{Z}_4$ vs $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$?

Count elements of order 2 in $\mathbb{Z}_4 \oplus \mathbb{Z}_4$:

(ord(a), ord(b))	# ways
2, 1	1
1, 2	1
2, 2	1
	3

G has 7 elts order 2, so $G \not\approx \mathbb{Z}_4 \oplus \mathbb{Z}_4$

$G \approx \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

More detail (Greedy alg Ch 11)

$\langle 7 \rangle \approx \mathbb{Z}_4$

$\parallel$

$\{1, 7, 49, 143\}$ $\cup$ $\quad \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \{e\}$

$\langle 199 \rangle = \langle -1 \rangle \approx \mathbb{Z}_2$ $\quad \{-1, -7, -49, -143\}$

$101 \notin \{1, 7, 49, 143, -1, -7, -49, -143\}$

$\langle 101 \rangle \approx \mathbb{Z}_2$

$$G = \underbrace{\langle 7 \rangle}_{\mathbb{Z}_4} \times \underbrace{\langle 199 \rangle}_{\mathbb{Z}_2} \times \underbrace{\langle 101 \rangle}_{\mathbb{Z}_2}$$

Proof of the Fundamental Theorem of Finite Abelian Groups

We'll sketch this to show that you've learned enough tools to be able to analyze this pretty complicated situation, and even classify one type of groups completely! Steps:

1. Prove that if G abelian, $|G| = p^m k$, and $\gcd(k, p) = 1$, then $G \approx H \oplus K$, where $|H| = p^m$ and $|K| = k$. This reduces problem to groups of prime power order.
2. Prove that if G abelian and $|G| = p^n$, and a is an element of largest possible order in G, then $G \approx \langle a \rangle \oplus K$ for some $K \leq G$. By induction, any finite abelian G is isomorphic to a product of cyclic groups of prime power order.
3. Prove that if G is abelian $|G| = p^n$, then there can be only one direct product of cyclic groups of order a power of p that is isomorphic to G.

Reducing to prime power order

Theorem

If G abelian, $\gcd(n, k) = 1$, and $|G| = nk$, then $G \approx H \oplus K$. Furthermore, if $n = p^m$, then $|H| = p^m$ and $|k| = K$.

Proof: Let

$$H = \{x \in G \mid x^n = e\}$$
$$K = \left\{x \in G \mid x^k = e\right\}$$

All subgroups normal in an abelian group, so remains to check that $H \cap K = \{e\}$ and $HK = G$.

Prime power order abelian groups are products of cyclic groups

Theorem

If G abelian and $|G| = p^n$, and a is an element of largest possible order in G, then $G \approx \langle a \rangle \oplus K$ for some $K \leq G$.

This is complicated! So we just sketch the idea. Proceeding by induction on $|G|$:

- Let a be an element of largest possible order in G.
- Choose $b \in G$ of smallest possible order such that $b \notin \langle a \rangle$. It can then be shown (through hard work) that $\langle b \rangle \cap \langle a \rangle = \{e\}$.
- Then $\overline{G} = G/\langle b \rangle$ is a group of order smaller than $|G|$, and $\overline{a}$ (the image of a in $\overline{G}$) is an element of maximum order in $\overline{G}$. By induction, $\overline{G} \approx \langle \overline{a} \rangle \times \overline{K}$ for some $\overline{K} \leq \overline{g}$. Pull that back to G to get $G \approx \langle a \rangle \oplus K$.

Cyclic products are unique

Theorem

If G is abelian and $|G| = p^n$, then there can be only one direct product of cyclic groups of order a power of p that is isomorphic to G.

Again, induction on $|G|$. Suppose

$$G \approx \mathbf{Z}_{p^{n_1}} \oplus \mathbf{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbf{Z}_{p^{n_k}}$$

and also

$$G \approx \mathbf{Z}_{p^{m_1}} \oplus \mathbf{Z}_{p^{m_2}} \oplus \cdots \oplus \mathbf{Z}_{p^{m_r}}.$$

The number of elements of order **dividing** p in $\mathbf{Z}_{p^{n_1}} \oplus \mathbf{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbf{Z}_{p^{n_k}}$ is:

So $k = r$, and can take factor group $G/(\mathbf{Z}_p \oplus \cdots \oplus \mathbf{Z}_p)$.