Math 322, lecture 20, 16/11/2017

**Last time:** $G$ simple of order $60 \Rightarrow G \simeq A_5$
(so $PSL_2(\mathbb{F}_5) \simeq A_5$)

**Q:** How did we know $\# P_2 = 4$?
**A:** $\# G = 60 = 2^2 \cdot 3 \cdot 5$, so $\# P_2 = 2^2$.

## ~~Abel~~ Finitely Generated Abelian Groups

### ① Finite abelian groups

Let $A$ be a finite abelian group of order $n$, let $p \mid n$. Then the $p$-Sylow subgp $A_p$ of $A$ is normal, hence unique.

HW: (a) $A = \langle \bigcup_{p \mid n} A_p \rangle$, (b) $A \simeq \prod_p A_p$

**Cor:** If $A$ has order $60$, $A \simeq P_2 \times P_3 \times P_5$, i.e.

$$\text{either } A \simeq C_4 \times C_3 \times C_5 \simeq C_{60}$$
or
$$A \simeq C_2 \times C_2 \times C_3 \times C_5 \simeq C_2 \times C_{30}$$

**Thm:** Let $A_p$ be a finite abelian $p$-group. Then $A_p$ is isomorphic to a pdt of cyclic $p$-gps, ~~uniquely up to the order~~ ~~for~~ of the factors of each size unique {with the number

Example: Group $(C_p)^k$ can factored many ways (choose a basis)

This group has $p^k$ elements, of which all but identity have order $p$: $(g_1, \ldots, g_k)^p = (g_1^p, \ldots, g_k^p)$.

On other hand, $C_{p^2}^k \times C_p^\ell \ncong C_p^{2k+\ell}$

Now $(g_1, \ldots, g_k, h_1, \ldots, h_\ell)$ has order $p^2$ iff one (or more) of the $g_i$ has order $p^2$.

<u>4:</u> $A = \prod_{p|n} A_p$, $g = g_{p_1} \cdots g_{p_k}$, $g_p \in A_p$

then the order of $g$ is pdt of orders of $g_p$.

Can put together info from each $A_p$ to get info in $A$.

<u>Conclusion:</u> If $A$ is a finite abelian gp then $A \cong \prod_{i=1}^r C_{p_i^{e_i}}$ with number of occurences of each $p_i^{e_i}$ unique

Return to uniqueness:

$$\mathbb{F}_p^2 = \operatorname{span}_{\mathbb{F}_p}\left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\} \underset{\phi}{=} \operatorname{span}_{\mathbb{F}_p}\left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right\}$$

Let $A = \mathbb{F}_p^2$, $B = \left\{\begin{pmatrix}x\\0\end{pmatrix} : x \in \mathbb{F}_p\right\}$, $C = \left\{\begin{pmatrix}0\\y\end{pmatrix} : y \in \mathbb{F}_p\right\}$

$D = \left\{\begin{pmatrix}z\\z\end{pmatrix} : z \in \mathbb{F}_p\right\}$, each $B \cong C \cong D \cong C_p$ as additive gps

and $A \cong B \times C \cong B \times D$

<u>Application of CRT:</u> Say $A \cong \prod_{i=1}^r C_{p_i^{e_i}}$

Define $d_1$ = product of highest powers of primes occuring

Ex: $A \cong C_9 \times C_3 \times C_{16} \times C_8 \times C_8 \times C_7$

$d_1 = 16 \cdot 9 \cdot 7$

Define $d_2$ = product of highest powers remaining

(Here $d_2 = 8 \cdot 3$)

Define $d_3$ = " " " "

(Here $d_3 = 8$)

Clear: $\cdots d_3 \mid d_2 \mid d_1$

The $d_i$ are called the "elementary divisors" of $A$.

By CRT, $A \cong C_{d_1} \times C_{d_2} \times C_{d_3} \times \cdots$

Thm: Any finite abelian group can be uniquely written in the form $A \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r}$ where $d_{i+1} \mid d_i$. Here the $d_i$ are unique.

Proofs: See notes, or Math 323

## Finitely Generated abelian groups

Let $A$ be a [finitely generated] abelian group

(e.g. $\mathbb{Z}^d$) $= \left\langle \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix} \right\rangle$

Ex: $\mathbb{Q}$ is not finitely generated as an abelian gp ("common denominator")

HW: $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ any finite set generates a cyclic subgp

same holds in $\mathbb{Q}/\mathbb{Z}$

---

Still, in $A$ a general abelian gp, $A_{tors} = \{a \in A \mid a \text{ has finite order}\}$

("torsion" = finite order)

Call $A$ "torsion free" if $A_{tors} = \{e\}$, "torsion" if $A = A_{tors}$

HW: If $A$ is abelian, $A_{tors}$ is a subgp

Thm: (1) Let $A$ be a torsion-free f.g. ab. gp. Then $A \cong \mathbb{Z}^d$ for some $d$.

(2) Let $A$ be f.g. ab gp. Then $A \cong \mathbb{Z}^d \times A_{tors}$, and $A_{tors}$ is finite.

Def: Call $d$ the rank of $A$

(Ex: if $\mathbb{Z}^d \cong \mathbb{Z}^e$ then $d = e$)

---

Examples: Let $E$ be a non-singular plane cubic with a rational pt. Examples $E$: $y^2 = x^3 + ax + b$ + pt at $\infty$ where $x^3 + ax + b = 0$ has no repeated roots

Say $a, b \in \mathbb{Z}$ or $\mathbb{Q}$.

If $k = \mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$, $E(k)$ = solutions $(x,y) \in k^2 + \{\infty\}$

note: If $P = (x,y) \in E(k)$, $(x,-y) \in E(k)$

set $-P = (x,-y)$ if $P = (x,y)$ $(-\infty = \infty)$

if $P, Q \in E(k)$, let $\ell$ be the line through $P, Q$.
let $Z$ be the third point in $\ell \cap E$ $(Z \in E(k))$

set $P + Q = -Z$.

Facts $(E(k), +)$ is an abelian group.

Examples: $x^3 + y^3 = 1$, $x^4 + y^4 = 1$

Thm: (Mordell-Weil): $E$ is def $/\mathbb{Q} \Rightarrow E(\mathbb{Q})$ is f.g. ab. gp.

[aside: $E(\mathbb{C}) \cong (\mathbb{R}/\mathbb{Z})^2$]

Question: What is rk $E(\mathbb{Q})$?

reduce coeffs mod $p$ (suppose $a, b \in \mathbb{Z}$)

say $\# E(\mathbb{F}_p) = p + 1 - a_p$ (Hasse: $|a_p| \le 2\sqrt{p}$)

Set $L(E;s) = \prod_p \frac{1}{(1 - a_p \cdot p^{-s} + p^{1-2s})}$ (converges if $\mathrm{Re}(s) > 3$)

Conj: $\mathrm{ord}_{s=1} L(E;s) = \mathrm{rk}\, E(\mathbb{Q})$ (Birch and Swinnerton-Dyer conj)