Lecture 12 Algebra I: Fund. Th^m f.g. ab. gps.

Another formulation: (Elementary Divisor decomp.)

Th^m: $|G| = n > 1$, $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ $p_1, \ldots, p_k$ The prime (distinct) divisors

1). $G \cong G_1 \times \cdots \times G_k$

where $|G_i| = p_i^{\alpha_i}$

2). For each $A \in \{A_1, \ldots, A_k\}$, $|A| = p^{\alpha}$,

$A \cong \mathbb{Z}_{p^{\beta_1}} \times \cdots \times \mathbb{Z}_{p^{\beta_\ell}}$

$\beta_1 \geq \beta_2 \geq \cdots \geq \beta_\ell \geq 1$, $\beta_1 + \cdots + \beta_\ell = \alpha$.

i.e., $\beta_1, \ldots, \beta_\ell$ are a partition of α.

3). The decomp. of 1+2 is unique.

the p^{β_i} are the elementary divisors of G.

N.B: The A_i are the Sylow subgps of G.

(unique as normal as G is abelian)

$\Rightarrow$ $G \cong$ Direct prod of Sylow subgps. (Proves 1+2?)

(we saw)

Ex: Abelian gps of order p^5: $p(5) = 7$

$5 = 5$, $5 = 4+1$, $5 = 3+2$, $5 = 3+1+1$, $5 = 2+2+1$, $5 = 2+1+1+1$, $5 = 1+1+1+1+1$.

Invariant factors

(1)

$\rightsquigarrow$ gps. $\mathbb{Z}_{p^5}$, $\mathbb{Z}_{p^4} \times \mathbb{Z}_p$, $\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$,

$\mathbb{Z}_{p^3} \times (\mathbb{Z}_p)^2$, $(\mathbb{Z}_{p^2})^2 \times \mathbb{Z}_p$, $\mathbb{Z}_{p^2} \times (\mathbb{Z}_p)^3$, $(\mathbb{Z}_p)^5$.

$\rightarrow$ 5^1, $4^1 1^1$, $3^1 2^1$, $3^1 1^2$, $2^2 1^1$, $2^1 3^1$, 1^5

so lots of gps of orders large powers of primes.

Hardy-Ramanujan: $p(n) \sim \frac{1}{4n\sqrt{3}} \cdot e^{\pi\sqrt{\frac{2n}{3}}}$.

Exercise: $p(n) \geq 2^{\sqrt{n}}$

So # of gps of order n $\Rightarrow$ # of abelian gps of order n

$\gg \frac{1}{n} \cdot e^{\pi\sqrt{\frac{2n}{3}}}$, n = ~~smallest divisor of n~~ largest power of a prime dividing n.

Ex: Gps of size $2^{10} = 1024$

$p(10) = 42$

$\rightsquigarrow$ 42 abelian gps.

Q: 50 Billion!

# of gps. total: 49,487,365,422

# of gps of size 2^{11} $\rightsquigarrow$ unknown! See Atlas!

Upper Bound: on # of gps.

Naive: n^{n^2} $\rightarrow$ # of cayley tables.

$\rightarrow$ Doesn't take into account Gp. laws, isomorphisms

Bette: (Fun plus nice review of Cayley Thm!!)

Th = # of gps of order $n \le n^{n \cdot \log_2 n} = O(n^{n^{1+\varepsilon}})$

Nice Practice!

Pf: First, a gp. can be generated by at most $\log_2 n$ elts.

Pause to ask them!

To see this, pick $g_1, g_2, \ldots$ s.t. ~~g_1 not the identity~~ $g_1 \neq e$, $g_{i+1} \notin \langle g_1, \ldots, g_i \rangle =: H_i$ (as long as possible).

$H_1 = \langle g_1 \rangle \neq 1$, so $|H_1| \geq 2$.

$H_{i+1} > H_i \Rightarrow |H_i| \mid |H_{i+1}| \Rightarrow |H_{i+1}| \geq 2|H_i|$

(ask them! ↙)

(↖ proper Lagrange; ↖ not =)

Induction $\Rightarrow |H_i| \geq 2^i$. Terminates by $i \leq \log_2 n$.

By Cayley, $G \hookrightarrow S_n$ (left reg. action)

images determined by $G = \langle g_1, \ldots, g_k \rangle$ (sufficient!)

images of $g_1, \ldots, g_k$

determined & choices of elts in S_n, $k \leq \log_2 n$.

$\Rightarrow (n!)^{\log_2 n}$ choices.

Now $n! = 1 \cdot 2 \cdot \ldots \cdot n \leq n \cdot \ldots \cdot n \leq n^n$.

$\Rightarrow$ # of gps $\leq n^{n \log_2(n)}$

Best known?: # of gps $\leq n^{c(\log_2 n)^2}$ constant c. ~~Fixed~~.

Equivalence of two fund. Th $\cong$.

Prop: $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff (m,n) = 1$

Follows by Chinese Remainder Th = (Ch Rmy Theorem)

Cor: If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$$

Can use to pass btw the 2.

Eg: $\mathbb{Z}_{30} \times \mathbb{Z}_{30} \times \mathbb{Z}_2$ (Elementary)

$\cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2$

Arrange: one row each prime. decreasing order.

$2^3\ 2^2\ 2^2$ $\quad 2\ 2\ 2^2\ 2^3$ $\quad 5^2\ 5$

$3\ 3\ 3$ $\quad\quad\quad 3\ 3\ 3$

$5^2\ 5$ $\quad\quad\quad\quad 2^3\ 2^2\ 2^2\ 2$

$\longrightarrow (\mathbb{Z}_{25} \times \mathbb{Z}_3 \times \mathbb{Z}_8) \times (\mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_2^2) \times (\mathbb{Z}_2)$

$= \mathbb{Z}_{600} \times \mathbb{Z}_{60} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (i.e., prod of cyclic)

Can obtain fr elem factors from any cyclic decomposition easily by Prop.

$\mathbb{Z}_6 \times \mathbb{Z}_{15} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

elem factors from invariant: also easy: just go:

$\mathbb{Z}_{600} \times \mathbb{Z}_{60}^{\times 2} \times \mathbb{Z}_6 \times \mathbb{Z}_2 = (\mathbb{Z}_{5^2} \times \mathbb{Z}_3 \times \mathbb{Z}_{2^3}) \times (\mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_{2^2}) \times (\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2) \times \mathbb{Z}_2$ (prime powers)

$\cong \mathbb{Z}_{25} \times \mathbb{Z}_5 \times \mathbb{Z}_8 \times \mathbb{Z}_4 \times (\mathbb{Z}_3)^3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times (\mathbb{Z}_2)^2$.

Prof Root loves to make stuff look complicated!

More on free gps. (# Scatter anywhere)

Make sense of presentation

Cut?
simple gp thy SVAS 2

S = Set of symbols, each s in S has a corresponding "inverse symbol" s^{-1} in S^{-1}

~~Free gp. F_S = {~~ ~~$T = S \cup S^{-1}$~~ $\rightsquigarrow T = S \cup S^{-1}$

Word .. Formal product of elts of T

empty word: no symbols.

ex: $S = \{a, b, c\}$

$T = \{a^{-1}, a, b^{-1}, b, c^{-1}, c\}$.

word: $a b^2 c^{-2} a^4 b^{-5} c$.

Can omit pairs $x x^{-1}$, can combine prods of powers use power rule for same symbol

$ab\ a b^2 c^{-2} a a^{-1} c^2 b \to a b^2 c^{-2} c^2 b \to a b^2 b = ab^3$

reduced word.

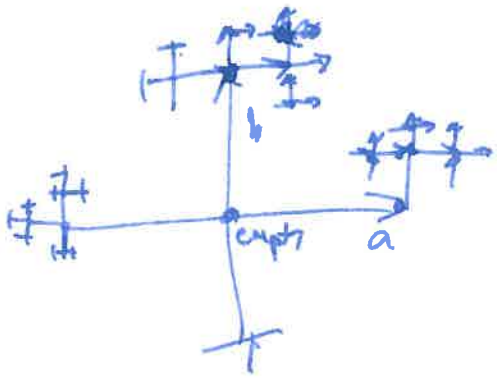
Free gp: {set of reduced words} under

operation of concatenation + reduction

Identity = empty word.

Picture: free gp. on $S = \{a, b\}$.

$F_{\{a,b\}}$ Cayley graph



(fractal-looking thing)

(look on Wikipedia for colored pic)

vertices = gp. elts.

→ mult by a ↑ mult. by b. edges: mult. by a or b

presentation $\langle S \mid r_1, \dots, r_n \rangle \cong F_{\{s_1,\dots,s_n\}} / \langle r_1, \dots, r_n \rangle$

hill.

$D_{2n} \cong F_{\{r,s\}} / \langle r^n, s^2, (sr)^2 \rangle$.

$sr = r^{-1}s \to srs = r^{-1} \to srsr = 1$.

(6) $(sr)^2 = 1$