1/19.

Algebra

21/01/2014

- Lecture 19
- Herbert Gangl
Homework: in next Tuesday
Website: ..... /~dmaohg/alg_EP14.htm.

- This term: Groups.
Ubiquitous in maths, arose from studying of (hidden) symmetries.
- Linear Algebra (matrix groups).
- Mathematical Physics
- Geometry (symmetry group of polygon).
- Complex Analysis (Möbius Transformation).

- Outline of topics:
- Revise notions & structural properties (of groups)
- Important families of groups (S_n, A_n, D_n): in detail.
(symm. gps., alter. gps., dihedral groups)
[For rings, have "prototypical" ring: $\mathbb{Z}$, here no such "prototypical" object, instead look at $\mathbb{I}$.
- Identify, distinguish gps. (homomorphism, isomorphism,
- Break up gp into "smaller" (more elementary) ones.
- Tying groups together.
- Make groups "visible" (group action).
- Classification results (for abelian groups: e.g. gps of order (prime)^2).
- More structural theorems ("orbit-Stabiliser Theorem", Cauchy's Theorem, Lagrange).

- Recall: Subgroup Criterion (→ tutorials this week).
For $(G, \cdot)$ group, have $H \subset G$ is a subgroup of $(G, \cdot)$ (with "$\cdot$" induced from G).
if
- H is non-empty
- $h_1, h_2 \in H \Rightarrow \underbrace{h_1 \cdot h_2}_{\in G} \in H$,
- $h \in H \Rightarrow h^{-1} \in H$.

Notation $H \leq G$ (shorthand for $(H, \cdot) \leq (G, \cdot)$)
(H is a subgroup of G)

Ex: $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ $n\mathbb{Z} < \mathbb{Z}$ (in fact this is an ideal of $\mathbb{Z}$)
$\{nk \mid k \in \mathbb{Z}\}$. (hence in particular a subgroup)

2. $(\mathbb{Z}^*, \cdot) < (\mathbb{Q}^*, \cdot) < (\mathbb{R}^*, \cdot) < (\mathbb{C}^*, \cdot)$
($\mathbb{Z}^*$: invertible elements; $\mathbb{Q}^*$: where $(A^*, \cdot)$ denotes the units of a ring $(A, +, \cdot)$.

eg. $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{Z}^* = \{1, -1\}$.

Claim: $(A^*, \cdot)$ is a group. (If a, b have inverses a', b' then $a \cdot b$ has inverse $b' \cdot a'$).

3. Obvious subgroups are $\{e\} < G$ (e: identity ele.), $G < G$.

4. diagonal matrices $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R}^* \right\} < GL_2(\mathbb{R})$.

- Each element $g \in G$ (group) generates a subgroup $\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\} \leq G$. This set can very well be finite.
Ex: $\sqrt{-1} = i \in \mathbb{C}$ $\rightsquigarrow \{i^k \mid k \in \mathbb{Z}\} \rightarrow$ has 4 elements
$i^k = i^{k+4}$.

- Def^n: More generally, for any subset $S \subset G$ (gp), the subgroup generated by S (in G) is the set of all the finite compositions of elements s_i in S and their inverses s_i^{-1}
Ex: $\langle \{\frac{1}{\pi}, 17, i\} \rangle = \{\pi^a \cdot 17^b \cdot i^c \mid a, b, c \in \mathbb{Z}\}$
for a non-commutative group $\langle a, b \rangle = \{a^{i_1} b^{j_1} a^{i_2} b^{j_2} \cdots a^{i_r} b^{j_r} \mid i_1 \cdots i_r, j_1, \ldots, j_r \in \mathbb{Z}, r \in \mathbb{Z}_{\geq 0}\}$

- Def^n: If the set $\langle g \rangle$ is a finite set, say of cardinality r, then we call r the order of g. Otherwise, g has infinite order.
Ex (Cont.): (1) $\{i^k \mid k \in \mathbb{Z}\} \rightarrow i$ has order 4 in $(\mathbb{C}^*, \cdot)$.
(2) More generally, $\zeta_m = e^{2\pi i/m}$ has order m.
(3) Identity element has order 1.
(4) The set $\langle -1 \rangle$ in $(\mathbb{Z}, +)$ is infinite, so the order of -1 is infinite.

- Def^n: The order of a group $(G, \cdot)$ is the cardinality of G.

Algebra

23/01/2014

- Lecture 20

- **Lagrange Theorem:**
G gp, $H < G$, Then (order of H) | (order of G). ($\#H | \#G$)
Proof: uses a notation of coset.

- Order of an element $g \in G$ ($= \#\langle\{g\}\rangle = \#\langle g \rangle$.) ($\#$ cardinality.)
Order of a group ($= \#\{\text{elements in } G\}$), notation $|G|$ (or $\#G$)

- Def^n: Let $H < G$. Then for any $g \in G$ call $gH = \{g \circ h \mid h \in H\}$.
the left coset of g w.r.t. H in G.
Notes: All left cosets w.r.t. H have the same cardinality
Proof: the map $\beta_g : H \to gH$ is a bijection
$h \to g \circ h$
Claim: • Left cosets (w.r.t. H in G) are either disjoint or coincide.
• Moreover, each element $g \in G$ lies in its own coset gH.
Upshot: G is the disjoint union of it's left cosets (w.r.t. H) and all cosets have the same cardinality.
"Think" G

In fact, the quotient $\frac{|G|}{|H|}$ ($\in \mathbb{Z}$) is equal to the no. of ~~differ~~ (different) cosets w.r.t. H.

Example: Consider the following six ~~facts~~ functions $\mathbb{C} \setminus \{0,1\} \to \mathbb{C} \setminus \{0,1\}$
$f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = \frac{x-1}{x}$, $f_4 = \frac{x}{x-1}$, $f_5 = \frac{1}{1-x}$, $f_6 = 1 - x$.
These form a group G under composition (of functions).
[Check: $f_3 \circ f_6(x) = f_3(1-x) = f_4(x) \cdots$]
The first two functions form a subgroup $H_{1,2} < G$.
The left coset w.r.t. $H_{1,2}$ are (apart from $f_1 H_{1,2}$ ($= H_{1,2}$ trivial coset)) $f_3 H_{1,2} = \{f_3, \underbrace{f_3 \circ f_2}_{f_6}\} = f_6 H_{1,2}$ and $f_5 H_{1,2} = \{f_5, \underbrace{f_5 \circ f_2}_{f_4}\} = f_4 H_{1,2}$
There are other ~~subgroups~~ subgroups like $\{f_1, f_4\}$ and $\{f_1, f_6\}$.

- Def^n: There's also the notion of a right coset (eg. $Hg = \{h \circ g \mid h \in H\}$)

Occasionally, left and right cosets agree. Then one has $gH = Hg$ but not necessarily $gh = hg$ $\forall h \in H$.

Example: (1) $H = 5\mathbb{Z} \leq \mathbb{Z}$ then $2 \in \mathbb{Z}$ has coset $2+5\mathbb{Z}$ which coincides with right coset $5\mathbb{Z}+2$. $= \{\dots, -3, 2, 7, \dots\}$

(2) In above example, take $H_{1,3,5} = \{f_1, f_3, f_5\}$, then $f_2 H_{1,3,5} = H_{1,3,5} f_2$ etc....

There is only one non-trivial coset (both left and right).

- Def^n: A subgroup $H < G$ is normal if left and right cosets agree $\forall g \in G$, $gH = Hg$. Denote this by $H \triangleleft G$.

Alternative (equal) def^n: $H < G$, H normal if $\forall g \in G$ $gHg^{-1} \in H$.

Example: (3) Scalar matrices $\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R} \setminus \{0\} \right\} \subset GL_2(\mathbb{R})$

(4) not normal; diagonal matrices $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R} \setminus \{0\} \right\}$

i.e. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \neq \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

- Importance of normal subgroups (see/compare with ideals)

In case $H \triangleleft G$, the cosets can be made into a group (cf. role of ideals inside rings). The so-called quotient group (of G by H).

Example: $n\mathbb{Z} \triangleleft \mathbb{Z}$ $(n > 0)$, cosets $\{n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \dots (n-1)+n\mathbb{Z}\}$

$(a+n\mathbb{Z}) +_q (b+n\mathbb{Z}) := (a+b)+n\mathbb{Z}$

$+_q$ quotient addition.

[Similarly for groups.

$$(g_1 H) \circ_q (g_2 H) = (g_1 g_2) H \quad]].$$

$$(gH)^{-1} := g^{-1} H.$$

Algebra 28/01/2014

- Lecture 21

- Example 0: If G is abelian (i.e. $gg'=g'g$ $\forall g,g'\in G$), then these agree "element wise". $gh=hg$ $\forall h\in H$, $g\in G$ so clearly $gH=Hg$.

Example 1: Set of functions $G=\{f_1,\dots f_6\}$ on $\mathbb{C}\setminus\{0,1\}$.
$f_1(x)=x$, $f_2(x)=\frac{1}{x}$, $f_3(x)=\frac{x-1}{x}$, eg $H_{1,2}=\{f_1,f_2\}<G$ but

$$f_3H_{1,2}=\{f_3f_1, f_3f_2\}=\{f_3, f_6\}\neq\{f_1,f_3,f_2f_3\}=\{f_1,f_3,f_4\}=H_{1,2}f_3$$
($f_3=f_3f_1$, $f_6=f_3f_2$, $f_4=f_2f_3$)

$\Rightarrow H_{1,2}$ is not a normal group.

Example 2: $H_{1,3,5}=\{f_1,f_3,f_5\}\lhd G$.
$f_2H_{1,3,5}=H_{1,3,5}H_2$
$f_4H_{1,3,5}=\vdots$
$f_6H_{1,3,5}=\vdots$
not "elementwise".
eg. $f_2f_3\neq f_3f_2$.

- Def^n: (i) Two elements $h,h'\in G$ are conjugate to each other if there is an $g\in G$ s.t. $ghg^{-1}=h'$ ($\Leftrightarrow gh=h'g$).

(ii) For an element $h\in G$, we call the set $ccl_G(h)=\{ghg^{-1}\mid g\in G\}$, the conjugacy class of h in G.

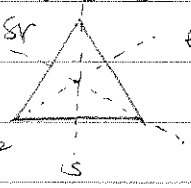
Note: A conjugacy class is never empty. ($h\in ccl_G(h)$.)

- Prop^n: Let $H<G$. Then H is normal in G $\Leftrightarrow$ H is a union of conjugacy classes in G.

Proof: "$\Rightarrow$" Suppose $H\lhd G$.
Then in particular for each $h\in H$, $ghg^{-1}\in H$ $\forall g\in G$.
Hence $ccl_G(h)=\{ghg^{-1}\mid g\in G\}\subset H=\bigcup_{h\in H}\{h\}\subset\bigcup_{h\in H}ccl_G(h)\subset H$
By "sandwiching" $\rightarrow$ "$\subset$" are "$=$".
"$\Leftarrow$" Suppose the subgroup H is the union of conjugacy classes.
To show: $gHg^{-1}=H$ $\forall g\in G$.
(equivalently $gHg^{-1}\subset H$ $\forall g\in G$).
but for fixed g
$$gHg^{-1}=\{ghg^{-1}\mid h\in H\}=\bigcup_{h\in H}\{ghg^{-1}\}\subset\bigcup_{h\in H}\{\tilde{g}h\tilde{g}^{-1}\mid\tilde{g}\in G\}=H$$
□

Example: Conjugate classes in D_3 = symmetry group of regular 3-gon.

D_3 has 6 elements $\{e, r, r^2, s, sr, sr^2\}$.



e = identity

r = rotation by $2\pi/3$

defining eq^{n}s: $D_3 = \langle r, s \mid r^3 = e, s^2 = e, srs^{-1} = r^2 \rangle$

Claim: There are 3 conjugacy classes in D_3.

(1) The identity forms a conjugacy class of its own $cc\ell_{D_3}(e) = \{e\}$.

(2) Conj. class of $cc\ell_{D_3}(r) = \{grg^{-1} \mid g \in D_3\}$

$= \{ere^{-1}, rrr^{-1}, r^2rr^{-2}, srs^{-1}, (sr)r(sr)^{-1}, (sr)^2r(sr)^{-2}\}$

$= \{r, r^2\}$ is also $cc\ell_{D_3}(r^2)$.

(3) $cc\ell_{D_3}(s) = \{s, sr, sr^2\} = \{ese^{-1}, rsr^{-1}, \dots\}$ has 3 elements $= cc\ell_{D_3}(sr) = cc\ell_{D_3}(sr^2)$

Upshot: Partitioning of $G = D_3$ into 3 conjugacy classes with 1, 2, 3 elements.

Prop^n: Conjugate elements in G have the same order.

(Compare $x \in G$, $gxg^{-1} \in G$)

$(gxg^{-1})^n = \underbrace{(gxg^{-1})(gxg^{-1}) \cdots (gxg^{-1})}_{n \text{ such}} = gx^ng^{-1}$

Now show $(gxg^{-1})^n = e \Leftrightarrow x^n = e$ (this implies claim).

Example. $G = D_3$, $Ord_{D_3}(r) = 3 = Ord_{D_3}(r^2)$ (i.e. $r^3 = e$)

$Ord_{D_3}(s) = 2 = Ord_{D_3}(sr) = Ord_{D_3}(sr^2)$ (i.e. $s^2 = e$)

$(sr)^2 = srsr = \underbrace{srs^{-1}}_{r^2}r = r^2 \cdot r = e$.

Note: A group G is abelian iff each conjugacy class consists of a single element.

Algebra 30/01/2014

- Lecture 22

- If $N \triangleleft G$ then G/N forms a group from last term.

- Defn: For $(G, \circ)$ $(G', *)$ groups, a map $\varphi: G \to G'$ is a group homomorphism if $\varphi(g_1 \circ g_2) = \varphi(g_1) * \varphi(g_2)$ for any $g_1, g_2 \in G$.

For $N \triangleleft G$, we have the canonical projection from G to G/N

$\pi_N: G \to G/N$

$g \to gN$

Note: π_N is a group homomorphism. $\leftarrow$ like $*$.

$\pi_N(g_1 \circ g_2) = (g_1 \circ g_2)N = (g_1 N) \circ (g_2 N) = \pi_N(g_1) \cdot \pi_N(g_2)$ $\forall g_1, g_2 \in G$

$\uparrow$ def^n of product in G/N

Note: π_N is surjective, and its kernel is N.

Surjectivity: for $X \in G/N$, ie $X = gN$ for some $g \in G$, $\pi_N(g) = gN = X$.

kernel π_N: $g \in G$ is $\in \ker \pi_N \iff \pi_N(g) =$ identity element in $G/N = eN = N$

- First isomorphism theorem for groups.

Let $\varphi: G \to H$ be a surjective gp homomorphism then

- $\ker(\varphi)$ is a normal subgroup
- $G/\ker(\varphi) \cong H$

Proof: Normality: $h \in \ker(\varphi)$, ie. $\varphi(h) = e_H$

Then $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = e_H$

Note: The map, denoting $N = e_H = \ker(\varphi)$

$G/N \to H$

$gN \to \varphi(g)$

Now check homomorphism & bijection.

- Defn: The centre $Z(G)$ of a group G is $Z(G) = \{x \in G \mid xg = gx \ \forall g \in G\}$.

Example 1: $Z(D_3)$ cannot contain r or s. (r and s do not commute) Similarly for r^2, rs, rs^2 $\Rightarrow Z(D_3) = \{e\}$.

Example 2: $Z(\langle g \rangle)$ is the whole $\langle g \rangle$

$\uparrow$ cyclic group generated by g

$g^k \cdot g^l = g^l \cdot g^k$

- Prop^n: The centre $Z(G)$ is a normal subgroup of G.

Proof: (1) Subgroup criterion.

(i) $x, y \in Z(G) \to xg = gx$, $yg = gy$ $\forall g \in G$.

$xy \in Z(G)$ means $(xy)g = g(xy)$.

since $(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$.

(ii) $x \in Z(G) \Rightarrow x^{-1} \in Z(G)$.

$xg = gx \; \forall g \Leftrightarrow (xg)^{-1} = (gx)^{-1} \; \forall g \Leftrightarrow g^{-1}x^{-1} = x^{-1}g^{-1} \; \forall g$.

(2) Normal subgroups.

for $z \in Z(G)$ consider $cl_G(z) = \{gzg^{-1} \mid g \in G\} = \{z\}$.

So in particular $Z(G)$ is the union of its elements (1) conjugacy classes.

Therefore $Z(G)$ is normal by previous prop^n.

Example 3: G abelian $\Rightarrow Z(G) = G$.

Example 4: $G = GL_2(\mathbb{R})$, then $Z(G) = \{\text{scalar matrices}\} = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R} \setminus \{0\}\right\}$.

- Direct product of groups. $(G, \circ_G)$ $(H, \circ_H)$

The direct (or cartesian) product of groups G, H is simply $G \times H = \{(g,h) \mid g \in G, h \in H\}$ with composition being induced from G and H. $(g_1, h_1) \circ_{G\times H} (g_2, h_2) = (g_1 \circ_G g_2, h_1 \circ_H h_2)$.

The identity is simply (e_G, e_H). The inverse of (g,h) is (g^{-1}, h^{-1}).

Example 1: $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{1},\bar{2})\}$.

Note that $(\bar{a}, \bar{b})$ here means $(a \bmod 2, b \bmod 3)$.

Example 2: $G \neq \{e\} \Rightarrow G \times G, G \times G \times G, \ldots \Rightarrow$ many different groups

Permutation groups

- Def^n: A permutation of a non-empty set X is a bijection from X to itself

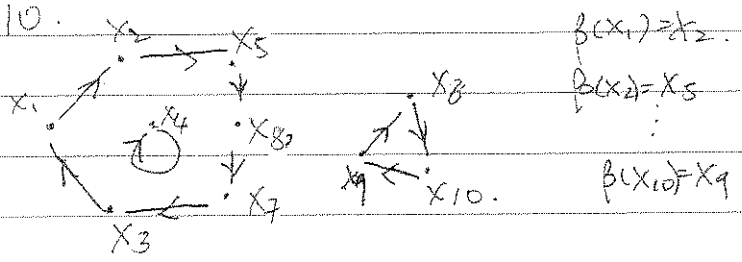
Algebra Lecture 22 continued.

- Note: For $X \neq \emptyset$ put $S_X = \{\beta : X \to X \mid \beta \text{ is a bijection}\}$.
  Fact: $(S_X, \circ)$ becomes a group because "$\circ$" denotes composition of functions.
  In particular, put $S_n := S_{\{1,\dots,n\}}$.

- Lemma: $|S_n| = n!$
  Proof: for first one have n choices, for second one have $n-1$ choices
  ..... $\Rightarrow$ Independent choices $\rightsquigarrow$ no. possibilities $= n(n-1)\cdots 1$

- Think of a (finite) set X in the plane, label its elements by $x_1, \dots x_n$

ie. $n=10$.



$\beta(x_1) = x_2$.
$\beta(x_2) = x_5$
$\vdots$
$\beta(x_{10}) = x_9$

Note: Each x_i is starting point of an arrow and an end point of an arrow, precisely one (each).
The arrows groups into disjoint (directed) "cycles"

Ex $\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 & x_{10} \\ x_2 & x_5 & x_1 & x_4 & x_8 & x_{10} & x_3 & x_7 & x_6 & x_9 \end{pmatrix}$ swap column

$\beta(x_1)$ $\beta(x_2)$ $\begin{pmatrix} x_1 & x_2 & x_5 & x_8 & x_7 & x_3 & x_4 & x_6 & x_{10} & x_9 \\ x_2 & x_5 & x_8 & x_7 & x_3 & x_1 & x_4 & x_{10} & x_9 & x_6 \end{pmatrix}$

Notation: $\begin{pmatrix} i_1 & i_2 & \dots & i_k \\ i_2 & i_3 & \dots & i_1 \end{pmatrix} \longleftrightarrow (i_1, \dots i_k)$ [all i_r $(1 \le r \le k)$ different]

Not unique! $(i_1 i_2 \cdots i_k) = (i_2 i_3 \cdots i_k i_1) = (i_3 i_4 \cdots i_k i_1 i_2)$ .... k different ways to write this.

Algebra 04/02/2014

- Lecture 23

- Specific bijections are called cycles (in fact k-cycles if they have k members).

Degenerate case: 1-cycle $\begin{pmatrix} i_n \\ i_n \end{pmatrix}$; only k-cycle that fixes an element.

Example: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ is not a cycle, but $\begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 1 \end{pmatrix}$ is.

- Building blocks for all permutations: are the 2-cycles (i_1, i_2) (with $i_1 \neq i_2$), also called transpositions.

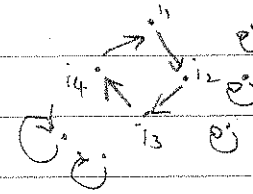
Two cycles are called disjoint if their "member sets" do not intersect.

Example: $(1\,2\,4)$ and $(3\,4\,5)$ are not disjoint (member sets have common element "4")

but $(1\,2\,4)$ and $(3\,5\,6)$ are disjoint cycles.

- Can compose cycles:

each cycle $(i_1 \dots i_k)$ can be extended in a unique way to a bijection of $\{1, \dots n\} \to \{i_1, \dots i_k\}$ by simply leaving the elements in the complement $\{1, \dots n\} \setminus \{i_1, \dots i_k\}$ unchanged.



Then to compose cycles means to simply compose the corresponding bijections obtained in this way.

Example: $n=4$.

Cycle notation. bijection.

$(1\,3\,2) \longleftarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \sigma_1$

$(3\,4) \longleftarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \sigma_2$

$\sigma_1 \sigma_2$ write σ_2 first $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$.

σ_1 second $\begin{pmatrix} 1 & 2 & 4 & 3 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ swap columns $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$

The composition $\sigma_1 \circ \sigma_2$ i.e. $(1\,3\,2)(3\,4)$ is given by $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ [simply drop middle rows].

in cycle form $(1\ 3\ 4\ 2)$

- Prop^n: (1). Any $\sigma \in S_n$ can be factored into a product of transpositions (i.e. 2-cycles)

(2) The parity (the no. of transpositions needed in such a factorisation is always the same) odd or even. (In particular, it is well-defined mod 2).

(3). A permutation with disjoint cycles of lengths $k_1, \dots k_m$ has order the lowest common multiple (lcm) $(k_1, \dots k_m)$

- Def^n: The sign of a permutation $\sigma \in S_n$ is defined as

$\operatorname{sgn}(\sigma) = (-1)^t$, where t denotes the no. of transpositions needed in a factorisation of σ. [Well-definedness guaranteed by Prop^n 1].

As we know (Q1, sheet 13).

$(i_1\ i_2 \cdots i_k) = (i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_2)$, hence

$\boxed{\operatorname{sgn}(\text{any } k\text{-cycle}) = (-1)^{k-1}}$

Example: $\sigma = \sigma_{k_1}\sigma_{k_2} \cdots \sigma_{k_r}$. Where σ_j are cycles of length k_j respectively has sign, $\operatorname{sgn}(\sigma) = (-1)^{(k_1-1)+(k_2-1)+\cdots+(k_r-1)}$

Example: $\operatorname{sgn}((1\,3\,4)(4\,5\,6\,2)) = (-1)^2(-1)^3 = -1$.

- Lemma: for $n \geq 2$, $\operatorname{sgn}: S_n \to \{\pm 1\}$ gives a surjective group homomorphism.

Proof: Suppose $\sigma_i\ (i=1,2) \in S_n$ can be written as a product of t_i transpositions.

To check homomorphism properties:

$\operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$

can write $\sigma_1\sigma_2$ as a product of t_1 transpositions for σ_1 with the t_2 transposition of $\sigma_2 \Rightarrow$ product has $t_1 + t_2$ transpositions.

Surjectivity:

There is at least one 2-cycle, say $(1\ 2)$ which has $\operatorname{sgn} = -1$.

24 Algebra 06/02/2015

- Lecture 24

- A cycle in S_n is of the form $(i_1, i_2, \dots i_k)$ $(k \le n)$ can be written as $\begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_k & j_1 & j_2 & \cdots & j_{n-k} \\ i_2 & i_3 & \cdots & i_1 & j_1 & j_2 & \cdots & j_{n-k} \end{pmatrix}$ [bijection notation]
Where $\{i_1, \dots i_k\} \cup \{j_1, \dots j_{n-k}\} = \{1, \dots n\}$.
From that bijection notation, retrieve cycle notation by drawing (dotted) parentheses whenever when ever the bottom entry & the top entry of successive columns do not agree.
Then can read off cycle notation from top (or bottom) row.
In case above, get: $(i_1, \dots i_k)(j_1)(j_2) \cdots (j_{n-k})$ or $(i_2 i_3 \dots i_k i_1)(j_1) \cdots (j_{n-k})$

- Convention: drop 1-cycles in cycle notation. Except in the case of a trivial bijection which we write as (1).

- Remark: A k-cycle has order k.

- Multiplying cycles from the right
Example: $(ab)(bc) = (bca)$.
$(bc)(ab) = (acb)$ second one first !!

- Lemma: Conjugating a transposition with another one gives again a transposition.

- Proposition (1) (2) (3) from last lecture:
Proof: (1) reduced to writing a given cycle in such a form, then compose respective results.
(2). Suppose there is $\sigma \in S_n$ which decomposes into both an even and an odd number of ~~trans~~ transpositions, say $\sigma = \tau_1 \cdots \tau_{2r}$, $\sigma = \tau_1' \cdots \tau_{2s+1}'$ (τ_i, τ_j' transpositions).
$\Rightarrow e = \sigma\sigma^{-1} = \tau_1 \cdots \tau_{2r} * \tau_{2s+1}' * \cdots \tau_1'$ is a product of an odd number of transpositions.
Suppose for a contradiction that
$e = \tau_1 \cdots \tau_{2m+1}$ (τ_i transpositions)

• Clearly $m>0$ (e is not a transposition)

• Up to ~~relabeling~~ relabeling, assume $\tau_1=(12)$.

Moreover, can assume that the 1st ℓ transp. $\tau_1,\dots\tau_\ell$ all contain "1" while $\tau_{\ell+1},\dots\tau_{2m+1}$ don't.

[If a,b,c are mutually different and $\neq 1$

$(ab)(c\,1)=(c\,1)(ab)$ and

$(a\,b)(b\,1)=(1\,a)(a\,b)$

$=(ab\,1)$ "]

$\Rightarrow \tau_1=(1\,a_1)\dots\tau_\ell=(1\,a_\ell)$ for some $a_i\in\{1,\dots n\}$.

Now these a_i cannot all be mutually different.

[otherwise $\tau_1\cdots\tau_\ell=(\cancel{a}\,1\,a_\ell\,a_{\ell-1}\cdots a_1)$, which does not ~~fix~~ leave "1" fixed ~~but~~ but the LHS($=e$) does as well as all the $\tau_{\ell+1},\dots\tau_{2m+1}$].

Hence suppose $a_i=a_j$ (some $1\le i<j\le\ell$)

So $\tau_1\cdots\tau_\ell=(1\,a_1)\cdots(1\,a_{i-1})(1\,a_i)(1\,a_{i+1})\cdots(1\,a_{j-1})(1\,a_j)\cdots(1\,a_\ell)$

$=(1\,a_1)\cdots(1\,a_{i-1})(a_i\,a_{i+1})(a_i\,a_{i+2})\cdots(a_i\,a_{j-1})(1\,a_{j+1})\cdots(1\,a_\ell)$.

As $(1\,a_i)(1\,a_i)=e$ $\forall i$, & $\underbrace{(1\,a_i)(1\,a_{i+1})(1\,a_i)}_{(a_i\,a_{i+1})}$

$\underbrace{(1\,a_i)(1\,a_{i+2})(1\,a_i)}_{(a_i\,a_{i+2})}$.

Now suppose the m was chosen minimally. Then we have found a shorter version of $e=\tau_1'\cdots\tau_{2m-1}'$ ✱.

Therefore, such an m does not exist. $\Rightarrow$ (2) ✱

- Def^n: The kernel of $\operatorname{sgn}: S_n\to\{\pm1\}$ is called the alternating group $A_n=\{\sigma\in S_n \mid \operatorname{sgn}(\sigma)=1\}$.

- Prop^n: (1) The group A_n is normal in S_n

(2) $\#A_n=\frac{n!}{2}$

(3) A_n is generated by 3-cycles.

Proof: (1) The kernel of a group homomorphism is normal (sub group)

(2) Any transposition multiplied to a given even permutation

Algebra lecture 24 continued

produces an odd permutation and vice versa $\Rightarrow$ this gives a bijection.

$$\{\text{even permutations in } S_n\} \longleftrightarrow \{\text{odd permutations in } S_n\}$$

$\uparrow$ contains half of everything in S_n.

(3). hint of proof: $\sigma = (i_1, j_1) \cdots (i_{2n}, j_{2n})$ can combine 2 successive ones to a product of 3-cycles.

Proof:

Write $\sigma = (i_1, j_1) \cdots (i_{2r}, j_{2r})$.

Now successively take two transpositions, each starting from the left, and combine them into 3-cycles.

Case 0: The 2 transpositions are the same $\rightarrow$ cancel.

Case 1: The two transpositions have precisely one member in common. $(ij)(jk) = (ijk)$.

Case 2: They are disjoint.

$$(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl).$$

~~Examples.~~

Algebra 11/02/2014

- Lecture 25

- Recall: families of cyclic groups $\mathbb{Z}_n$, dihedral groups D_n, symmetric groups S_n, alternating groups A_n.

- Each $\sigma \in S_n$ can be written as a product of disjoint cycles, eg. $\sigma_0 = (173)(2456)(89)$.

[Not unique for each k-cycle have k ways to write it; moreover, disjoint cycles commute. Above σ_0 can be written in ~~3·4·2·3~~ $3 \cdot 4 \cdot 2 \cdot 3$ ways].

Each k-cycle in turn can be written in terms of $(k-1)$ transpositions.
[Not unique: $e = (12)(12) = (12)(34)(12)(34)$; etc].
Large ambiguity ~~of~~ to write the same permutation.
But: at least the parity of the number of transpositions is well-defined

$\text{sgn}: S_n \to \{\pm 1\}$
This leads to homomorphism with kernel $A_n = \{\sigma \in S_n \mid \text{sgn}(\sigma) = +1\}$ (or σ even)

- Examples: {subgroup of A_n, S_n}.

(1) "Klein 4-group" V_4.

identity ↓

$\langle (12)(34), (13)(24) \rangle = \{(1), (12)(34), (13)(24), (14)(23)\}$

Variant of notation: $\{e, a_1, a_2, a_3\}$, $a_j^2 = e$, $a_i a_j = a_k$ where $\{i, j, k\} = \{1, 2, 3\}$.

(2) Subgroups in S_4 which are not in A_4.

$\langle (12) \rangle \subset S_4$
$\langle (1234) \rangle \subset S_4$ } but not $\subset A_4$.

$\langle (12), (123) \rangle$ generates a subgp of S_4, isomorphic to S_3.
$\langle r = (1234), s = (12)(34) \rangle$ satisfy $r^4 = e$, $s^2 = e$, $srs^{-1} = r^{-1}$
So precisely the relations in D_4.

- Distinguish and identify groups

"Distinguish" (ie show they are non-isomorphic)

- An isomorphism preserves in particular:

- Numerical Invariants:
  The order of the group G.
  The set of possible orders of elements in G (with multiplicities).
  The size of its centre.
- Structural invariants:
  Abelian vs. non-abelian.
  The property of having normal subgroups.

Examples:

(1). $\mathbb{Z}_6$ and D_3 are both of order 6, but $\mathbb{Z}_6$ has an element of order 6, D_3 does not $\Rightarrow \mathbb{Z}_6 \not\cong D_3$.

S_3 also has order 6.

orders of elements $\underset{①}{1}, \underset{③}{2}, \underset{②}{3}$. } indeed $D_3 \cong S_3$.

$D_3 = \{e, r, r^2, s, sr, sr^2\}$

order $1 \quad 3 \; 3 \quad 2 \; 2 \; 2$

Proposition: Two cyclic groups of the same order are isomorphic.

Proof: $G = \langle g \rangle$, $H = \langle h \rangle$, $\#G = \#H$. Then $\varphi: G \to H$

$g^r \mapsto h^r \quad \forall r \in \mathbb{Z}$.

Need to check:

· Well-definedness · Surjectivity · Injectivity · homomorphic properties

Use $g^r = g^s \Leftrightarrow \#G \mid r-s \Leftrightarrow h^r = h^s$

Q: How to recognise a group as a direct product of 2 smaller subgps?

Example: $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

[seen as rings! Forget ring multiplication to get isomorphic as groups]

More generally, whenever $\gcd(m,n) = 1$ then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

$(a \bmod m, a \bmod n) \longleftarrow\!\shortmid (a \bmod mn)$

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

More conceptual way to identify group with a direct product.

Notation: for a group $(G, \circ)$ and two subsets $E_1, E_2 \subset G$ define

$E_1 \circ E_2 = \{h_1 \circ h_2 \mid h_1 \in E_1, h_2 \in E_2\}$

Algebra lecture 25 continued

- Theorem (Criterion):

Let H, K be subgroups of G st. the following 3 conditions are satisfied:

(1) $H \circ K = G$

(2) $H \cap K = \{e\}$

(3) $hk = kh$ for any $h \in H, k \in K$.

Then $G \cong H \times K$

Proof: $\varphi: H \times K \to G$ by $\varphi((h,k)) = h \circ k$

Then (1) → surjectivity

(2) → injectivity

(3) homomorphic properties

- Example 1: $V (= V_4) = \{e, a_1, a_2, a_3\}$

s.t. $a_i^2 = e$ & $a_i a_j = a_k$ whenever $\{i,j,k\} = \{1,2,3\}$

Show $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Each group of order 2 is isomorphic to $\mathbb{Z}_2$.

multiplication eg.

$\circ$	e	a
e	e	a
a	a	e

Put $H_i = \{e, a_i\} < G = \langle a_i \rangle$, of order 2.

Let $H = H_1$, $K = H_2$ then

(1) $H \circ K = \{e \circ e, e \circ a_2, a_1 \circ e, a_1 \circ a_2\}$

$= \{e, a_2, a_1, a_1 a_2\} = V$

(2) $H \cap K = H_1 \cap H_2 = \{e\}$.

(3) Only need to check $a_1 \circ a_2 = a_2 \circ a_1 (= a_3)$ ✓

(others are trivial)

$\Rightarrow V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

- Example 2: Claim $D_6 \cong \mathbb{Z}_2 \times D_3$.

$D_6 = \langle r, s \mid r^6 = e, s^2 = e, srs^{-1} = r^{-1} \rangle$

$= \{r^i s^j \mid 0 \le i \le 5, 0 \le j \le 1\}$

Choose $H = \langle r^3 \rangle$, is order 2 $((r^3)^2 = r^6 = e)$.

and $K = \langle r^2, s \mid r^6 = e, s^2 = e, \underbrace{srs^{-1} = r^{-1}}_{sr^2s^{-1} = r^{-2}} \rangle$

put $\tilde{r} = r^2$.

$K = \langle \tilde{r}, s \mid \tilde{r}^3 = e, s^2 = e, s\tilde{r}s = \tilde{r}^{-1} \rangle \cong D_3$.

Criterion: check

(1) $H \circ K = D_6$.

$\Leftrightarrow H \circ K = \{e, r^3\} \cdot \{e, \tilde{r}, \tilde{r}^2, s, \tilde{r}s, \tilde{r}^2 s\}$

(use $\tilde{r} = r^2$) $= \{e, r, r^2, \cdots r^5, s, rs, \cdots r^5 s\}$.

$= D_6$ ✓.

(2) To show $r^3 \notin K$.

(3) To check $hk = kh$ $\forall h \in H, k \in K$.

to check: r^3 commutes with any $k \in K$.

$r^3 (r^i) = (r^i) r^3$.

$r^3 (r^i s) = (r^i s) r^3$. $[\![(r^3)^{-1} = r^3]\!]$.

$\Rightarrow$ Claim.

Algebra 13/02/2014.

- Lecture 26.

Groups as (subgroups of) permutation groups

- Next aim: "uniformize" groups, write each group as a (subgroup of) some permutation group.

- Example (geometric).

- Theorem: The group of rotations (in $\mathbb{R}^3$) of the cube is isomorp to S_4

i.e. centre of mass.

Proof: Rotations → think: barycenter = origin, vertices on a sphere (around origin) ∎.

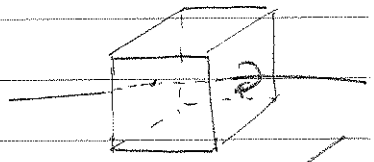
Each rotation has a rotation axis. If each rotation correspond to matrix in $SO_3(\mathbb{R})$ (Special ie det = 1 Orthogonal) has ≠1 eigenvalues = 1. line through corresponding eigenvector gives rotation axis.

Possibilities: rotation axis through two opposite.

(i) face centres by angle $\pi/2, \pi, 3\pi/2$.

This gives $\frac{\#\{\text{faces}\}}{2} \times \#\{\text{non-trivial rotations}\}$

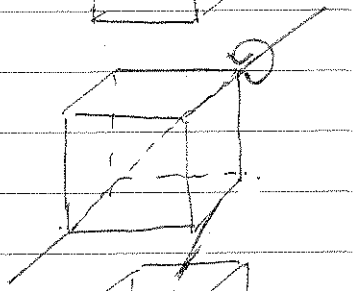
$= 6/2 \times 3 = 9$ such



(ii) Vertices by angles $\frac{2\pi}{3}, \frac{4\pi}{3}$.

Gives $\frac{\#\{\text{vertices}\}}{2} \times \#\{\text{non-triv rotation}\}$

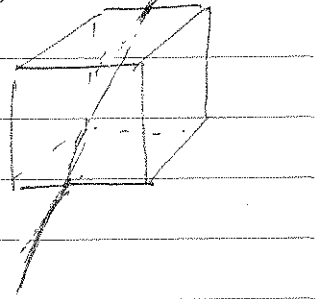
$= 8$ such.



(iii) edge centres

gives $\frac{\#\{\text{edges}\}}{2} \times \#\{\text{non-trivial rotation}\}$

$= \frac{12}{2} \times 1 = 6$.



$9+8+6 = 23$ non-trivial rotations.

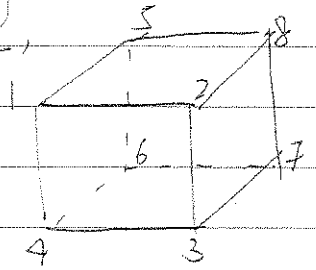
& "trivial" rotation → 24 elements.

Now use either $V = \{\text{vertices}\}$ $E = \{\text{edges}\}$ $F = \{\text{faces}\}$

Realise these symmetries by tracing what happens on the

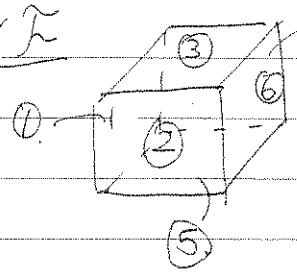
(labelled) sets of V, E, F.

For V,



$(1\,5\,8\,4)(2\,6\,7\,3) \in S_V \cong S_8$.

For F



$(1)(2\,3\,4\,5)(6) \in S_F \cong S_6$

For E . . . . . $\in S_E \cong S_{12}$.

-Theorem (Cayley) Each group $\#(G, \circ)$ is isomorphic to a (subgp of) a permutation group.

Algebra 18/02/2014

- Lecture 27

- Theorem (Cayley):
Each group $(G,\cdot)$ is isomorphic to a subgroup of some permutation group S_X, for some set X.
In fact, we can choose X to be G.

Proof: Crucial idea: attach to each $g \in G$ a permutation L_g ('left translation') $L_g : G \to G$.
$h \to gh$.

Claim 1: L_g is a permutation, ie is bijective.
(a) Injectivity: $L_g(h) = L_g(h')$ To show $h = h'$.
$\hookrightarrow gh = gh' \xrightarrow[\text{by } g^{-1}]{\text{mult.}} h = h'$ ✓.

(b) Surjective: for $k \in G$, need to find $h \in G$ s.t. $L_g(h) = k$.
take $h = g^{-1}k (\in G)$, then $L_g(h) = L_g(g^{-1}k) = g(g^{-1}k) = k$ ✓.

Now put $G' = \{L_g \mid g \in G\}$ (a set).

Claim 2: G' is a group (binary operation: compositions of fns).
Clearly $G' \subset S_G$.
(a) G non-empty: to e attach $L_e \in G'$.
$L_e(h) = e \cdot h = h \ \forall h \in G \Rightarrow L_e$ is identity.
(b) for two elements in G' can find $g, h \in G$ to write them as L_g and L_h, respectively. so composition give. $L_g \circ L_h$; want to write it as L_k for some $k \in G$. Take $k = gh$, then. $L_g \circ L_h(a)$
$= L_g(ha) = g(ha) = (gh)a = L_{gh}(a) \ \forall a \in G$.
(c) G' closed under taking inverses. Suffices to show $(L_g)^{-1} = L_{g^{-1}}$
[$L_{g^{-1}} \circ L_g(a) = L_{g^{-1}}(ga) = g^{-1}ga = a = L_e(a)$].
$\Rightarrow$ Subgroup criterion $\Rightarrow$ claim 2 ✓.

In the proof we have shown that:
$\psi : G \to G'$.
$g \to L_g$ is a homomorphism (of groups) — specify
[$\psi(gh) = \psi(g) \circ \psi(h)$].

Claim 3: φ is in fact an isomorphism.

To show: φ is bijective.

(a) Surjective: by construction of G'.

(b) Injective: $\varphi(g)=\varphi(h) \Rightarrow g=h$.

$L_g = L_h$ ie $L_g(a)=L_h(a)$ $\forall a \in G$.

ie. $ga=ha$ $\forall a \in G$.

in particular, for $a=e \rightsquigarrow g=h$. ∎

Example: Let V = Klein-4 group $=\{e, a_1, a_2, a_3\}$ where $a_i^2=e$, $a_i a_j = a_k$ $\{i,j,k\}=\{1,2,3\}^3$.

Want to show: V is isomorphic to a subgroup of S_X. where $X=\{x_1=e, x_2=a_1, x_3=a_2, x_4=a_3\}$.

Proof of Cayley's Theorem suggests to map a_i to L_{a_i} $(i=1,2,3)$

For $i=1$, $a_1 = L_{a_1}$: $x_1=e \longmapsto a_1 e = x_2$.

$x_2=a_1 \longmapsto a_1 a_1 = x_1$

$x_3=a_2 \longmapsto a_1 a_2 = x_4$

$x_4=a_3 \longmapsto a_1 a_3 = x_3$

ie. L_{a_1} as a permutation is $(x_1 x_2)(x_3 x_4)$. Similarly, $L_{a_2} \leftrightarrow (x_1 x_3)(x_2 x_4)$, $L_{a_3} \leftrightarrow (x_1 x_4)(x_2 x_3)$.

By the proof of the theorem (Claim 2). to V.

$G' = \{L_e, L_{a_1}, L_{a_2}, L_{a_3}\}$ forms a group isomorphism

- Last week's example of rotations of a cube (say R = rotation group) indicated homomorphisms.

$R \to S_X$ with $X=\{$vertices of cube$\}$ $\#=8$

or $=\{$edges of cube$\}$ $\#=12$

or $=\{$faces of cube$\}$ $\#=6$

Aside: There is an even more economical way to write R as a permutation group: $X=\{$main diagonals of cube$\}$ $\#=4$ incl.

- Defn: An action of a group G on a (non-empty) set X is a homomorphism: $\varphi: G \longrightarrow S_X$. In other words, assign a permutation $\varphi(g)$ (of X) for each $g \in G$ s.t. $\varphi(g)\varphi(h)=\varphi(gh)$.

We also write that G acts on X.

Algebra lecture 27 continued

Note: In the def^n, we assume φ neither to be injective or surjective

- Example: Two very different actions of $(\mathbb{Z},+)$ on $\mathbb{R}$.

(1) Let $(\mathbb{Z},+)$ act on $\mathbb{R}$ by left-translation.

ie. $\psi: \mathbb{Z} \longrightarrow S_{\mathbb{R}}$

$$n \longrightarrow \{L_n: \mathbb{R} \to \mathbb{R},\ r \to n+r\}.$$

group action: For any $m,n \in \mathbb{Z}$

$$\psi(n)\circ\psi(m)(r) = \psi(n)(m+r) = n+(m+r).$$

$$\psi(n+m)(r) = (n+m)+r \quad \text{// associativity of "+" in } \mathbb{R}.$$

(2) Let $(\mathbb{Z},+)$ act by multiplying (-1) or $(+1)$.

$\psi: \mathbb{Z} \longrightarrow S_{\mathbb{R}}$

$$n \longrightarrow \{M_n: \mathbb{R} \to \mathbb{R},\ r \to (-1)^n r\}.$$

Group action: notion of group action ie. a homomorphism

$$\varphi: G \longrightarrow S_X.$$

- Halftime Resumé

- families of groups: $\mathbb{Z}_n$ (cyclic), D_n (dihedral), S_n (symmetric), A_n (alternating)
- Subgroups, normal or not, quotient groups.
- Direct product of groups.
- Structure preserving maps (homomorphism)
- "Uniformisation" via permutation of groups (Cayley's Theorem)
- Now visualise groups by observing what it does to appropriately chosen sets.

Algebra 20/02/2014

-Lecture 28.

-Example 1: $\mathbb{Z}$ acting on $\mathbb{R}$ by left translation $\varphi: \mathbb{Z} \to S_{\mathbb{R}}$, $n \to L_n$, where $L_n: \mathbb{R} \to \mathbb{R}$, $r \to n+r$.

Example 2: $\mathbb{Z}$ acting on $\mathbb{R}$ by multiplication of $\begin{cases} 1 & \text{if } n \in \mathbb{Z} \text{ even} \\ -1 & \text{if } n \in \mathbb{Z} \text{ odd} \end{cases}$

$\varphi: \mathbb{Z} \to S_{\mathbb{R}}$, $n \to M_n$, $M_n: \mathbb{R} \to \mathbb{R}$, $r \mapsto (-1)^n r$

[To check φ homomorphism use $(-1)^{m+n} = (-1)^m (-1)^n$].

Example 3. $\mathbb{Z}_4$ acting of sets of vertices $\{v_1, \dots, v_8\}$ of a cube

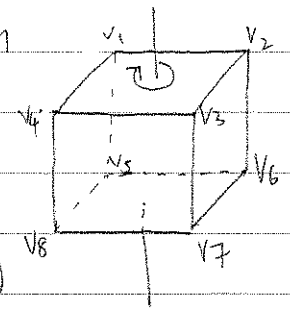
Let r be rotation around axis (top/bottom face centres) by angle $\pi/2$ → rotation of the cube

Then let $X: \mathbb{Z}_4 \to R \to S_{\{v_1,\dots,v_8\}}$.

$\bar{1} \to r$, $r \to (v_1 v_2 v_3 v_4)(v_5 v_6 v_7 v_8)$

$\bar{2} \to r^2$, $r^2 \to (v_1 v_3)(v_2 v_4)(v_5 v_7)(v_6 v_8)$

$\bar{3} \to r^3$, $r^3 \to (v_4 v_3 v_2 v_1)(v_8 v_7 v_6 v_5)$



In general, $\bar{k} \to r^k$

Note: We could also map $\bar{1}$ to r^2 hence $\bar{2}$ to $r^4 = e$

ie. get non-trivial kernel for map $G \to S_X$.

-Defn: Let $\varphi: G \to S_X$ be an action (of group G on set X). Then $\forall x \in X$ define:

(1) $G(x) = \{\varphi(g)(x) \mid g \in G\} \subset X$ the G-orbit of x inside X

(2) $G_x = \{g \in G \mid \varphi(g)(x) = x\} \subset G$ the stabiliser of x inside G.

-Lemma: Let $\varphi: G \to S_X$ be a group action. Then G_x is a subgroup of G

Proof: G_x is non-empty. [Since φ is a homomorphism, we have $\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e) \Rightarrow \varphi(e)$ is the identity permutation].

In particular, $\varphi(e)(x) = x$ ie. $e \in G_x$.

- for $g,h \in G_x$ have $gh \in G_x$

[I want: $\varphi(gh)(x) = x$. have: $\varphi(gh)(x) = (\varphi(g)\varphi(h))(x) = \varphi(g)(\underbrace{\varphi(h)(x)}_{=x,\ h\in G_x}) = \underbrace{\varphi(g)(x)}_{=x,\ g\in G_x} = x$].

- for $g \in G_x$, have $g^{-1} \in G_x$

[$\varphi(g^{-1})(x) = \varphi(g^{-1})(\varphi(g)(x)) = \varphi(e)(x) = x$].

$\Rightarrow$ Lemma

- Examples (revisited)

(1) $G = \mathbb{Z}$ acting on $\mathbb{R}$ by left translation. Find orbits & stabilisers under this action.

Fix $x \in X$. Its G-orbit is

$G(x) = \{\varphi(g)(x) \mid g \in G\} = \{L_n(x) \mid n \in \mathbb{Z}\} = \{n+x \mid n \in \mathbb{Z}\}$.

Its stabiliser is

$G_x = \{g \in G \mid \varphi(g)(x) = x\} = \{n \in \mathbb{Z} \mid L_n(x) = x\} = \{n \in \mathbb{Z} \mid n + x = x\}$

$= \{0\}$

(2) $G = \mathbb{Z}$ acting on $\mathbb{R}$ by multiplication of ± 1.

$M_n : \mathbb{R} \to \mathbb{R}$, $r \mapsto (-1)^n r$. Fix $x \in X$. Its G-orbit is

$G(x) = \{M_n(x) \mid n \in \mathbb{Z}\} = \{(-1)^n x \mid n \in \mathbb{Z}\} = \{x, -x\}$

Cases: 1) $x = -x$ ie. $x = 0 \Rightarrow G(0) = \{0\}$ 1 element.

2) $x \neq -x$ ie $x \neq 0 \Rightarrow G(x) = \{x, -x\}$ 2 elements.

Stabilisers are:

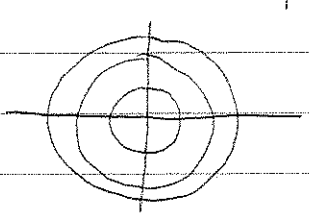
$G_x = \{n \in \mathbb{Z} \mid M_n(x) = x\} = \{n \in \mathbb{Z} \mid (-1)^n x = x\}$

$= \{n \in \mathbb{Z} \mid n \text{ even}\} = \begin{cases} 2\mathbb{Z} & x \neq 0. \\ \mathbb{Z} & x = 0 \end{cases}$

Group action of $\mathbb{R}$ on $\mathbb{C}$ given by

$r \in \mathbb{R} \longrightarrow$ multiply by e^{ir} ie. $z \longmapsto e^{ir} z$

Orbits



look like orbits of planets.

Algebra 25/02/2014

-Lecture 29

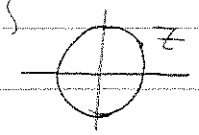
-Recall: The notion of a group action (ie. a group homo $\varphi: G \to S_X$) gives rise, for each $x \in X$ to:
- Its G orbit $G(x) = \{\varphi(g)(x) \mid g \in G\} \subset X$.
- Its stabiliser.

-Example: $\mathbb{R}$ acting on $\mathbb{C}$ as follows. $\varphi: \mathbb{R} \to S_{\mathbb{C}}$, $r \to E_r$. $E_r: \mathbb{C} \to \mathbb{C}$, $z \to e^{ir}z$

orbits of $z \in \mathbb{C}$: Distinguish (1) $z = 0$.

$G(0) = \{\varphi(r)(0) \mid r \in \mathbb{R}\} = \{e^{ir} \cdot 0 \mid r \in \mathbb{R}\} = \{0\}$

(2) $z \neq 0$. $G(z) = \{e^{ir} z \mid r \in \mathbb{R}\} = \{w \in \mathbb{C} \mid |w| = |z|\}$.



Stabilisers (1) for $z = 0$.

$G_0 = \{r \in \mathbb{R} \mid e^{ir} \cdot 0 = 0\} = \mathbb{R}$.

(2) for $z \neq 0$. $G_z = \{r \in \mathbb{R} \mid e^{ir} \cdot z = z\} = \{2\pi n \mid n \in \mathbb{Z}\} \cong \mathbb{Z}$.

NOTE: Notation: We'll mostly drop "φ" from the notation of a group action, for example $\varphi(g)(x)$ replaced by $g(x)$, similarly $\varphi(h)\varphi(g)(x)$ replaced by $h(g(x))$ and

$G_x = \{g \in G \mid g(x) = x\}$.

-Propⁿ: Let G act on X, $\varphi: G \to S_X$. Then the distinct orbits partition X. ie: (1) each orbit is a non-empty subset of X

(2) the union of all orbits is X.

(3) orbits either are disjoint or coincide.

Proof: (1) Note $\varphi(e)$ is the identity permutation and so $x \in G(x)$

(2) $X = \{x \mid x \in X\} \subset \{G(x) \mid x \in X\} \subset X$

(3) Suppose $z \in G(x) \cap G(y)$. ie. $z = g_1(x) = g_2(y)$.

then $x \in G(y)$ $x = g_1^{-1}(z) = g_1^{-1}(g_2(y)) = g_1^{-1}g_2(y)$. $\in G$

Claim: claim: in fact, $G(x) \subset G(y)$.

Suppose we $G(x)$ ie. $w = g_3(x)$. then $w = g_3(g_1^{-1}g_2(y)) = (g_3 g_1^{-1} g_2)(y)$ $\in G$

By reverse, get $G(y) \subset G(x) \Rightarrow G(x) = G(y)$

Remark: To be in the same orbit (under some group action) is an equivalence relation.

- Two distinguished group actions of G on itself, i.e. $X=G$.

(1) Look at proof of Cayley's Theorem, $g\in G$ acts by left translation: $L_g: G\to G$, $h\to gh$. old notation: $L_g(h)=gh$. new notation: $g(h)=gh$.

- Orbit of $x\in X=G$.

$G(x)=\{g(x)\,k : g\in G\}=\{gx \mid g\in G\}=G$

- Stabiliser

$G_x=\{g\in G \mid g(x)=x\}=\{g\in G \mid gx=x\}=\{e\}$.

(2) ~~Groups~~ G acts on itself via conjugation:

$\varphi: G\to S_G$ where $\varphi(g)(h)=ghg^{-1}$ (new notation: $g(h)=ghg^{-1}$)
$g\to \varphi(g)$

claim: This gives a homomorphism

$\varphi(gg')(h)=(gg')h(gg')^{-1}$ (=x)

$\varphi(g)(\varphi(g')(h))=\varphi(g)(g'hg'^{-1})=g(g'hg'^{-1})g^{-1}$

- Lemma: Let G act on itself by conjugation. Then for any $x\in G$, its orbit $G(x)$ coincides with the conjugacy class of x inside G.

Proof: Compare defn: $Cl_G(x)=\{gxg^{-1} \mid g\in G\}$

Here an orbit (under group action by conjugation) is

$G(x)=\{g(x) \mid g\in G\}=\{gxg^{-1} \mid g\in G\}$ ✓

- Examples:

(0) The conjugacy class of e is $\{e\}$.

(1) In an abelian group, all conjugacy classes have size 1.

2) Let S_3 act on itself by conjugation.

Orbits = conjugacy classes: ① $\{e\}$, ③ $\{(12),(23),(31)\}$, ② $\{(123),(321)\}$

Stabilisers: ⑥ S_3

$G_{(12)}=\langle(12)\rangle$
$G_{(23)}=\langle(23)\rangle$
$G_{(31)}=\langle(31)\rangle$
} ②, resp.

$G_{(123)}=\langle(123)\rangle$
$G_{(321)}=\langle(321)\rangle$
③

Algebra 27/02/2014

- Lecture 30

- Recall: group action, orbits, stabilisers.

- Example(3): Let the dihedral group D_5 act on itself by conjugation. Determine its orbits, i.e. conjugation classes.

[Write $D_5 = \langle r, s \mid r^5 = e = s^2, srs^{-1} = r^{-1} \rangle$
$= \{ r^i s^j \mid 0 \le i \le 4, 0 \le j \le 1 \}$]

Two cases: (α) $cc\ell_{D_5}(r^i)$, $0 \le i \le 4$ (β) $cc\ell_{D_5}(r^i s)$

(α) fix i $cc\ell_{D_5}(r^i) = \{ r^k r^i (r^k)^{-1} \mid 0 \le k \le 4 \} \cup \{ (r^k s) r^i (r^k s)^{-1} \mid 0 \le k \le 4 \}$
$= \{ r^i \} \cup \{ r^{-i} \}$.

[$r^k s r^i s^{-1} r^{-k} = r^k r^{-i} r^{-k} = r^{-i}$].

(β) $cc\ell_{D_5}(r^i s) = \{ r^k (r^i s) r^{-k} \mid 0 \le k \le 4 \} \cup \{ r^k s (r^i s)^{-1} r^{-k} \mid 0 \le k \le 4 \}$
$= \{ r^{2k+i} s \mid 0 \le k \le 4 \} \cup \{ r^{2k-i} s \mid 0 \le k \le 4 \}$
$= \{ r^j s \mid 0 \le j \le 4 \}$.

Summary: The conjugacy classes of D_5 are $\{e\}$ (i=0), $\{r^2, r^{-2}\}$ (i=2), $\{r, r^{-1}\}$ (i=1), $\{ r^j s \mid 0 \le j \le 4 \}$ (5) & $G = D_5$.

Stabilisers: D_5 (N), $G_r = (D_5)_r = \langle r \rangle = G_{r^{-1}} = \langle r^{-1} \rangle = \langle r \rangle$, $G_{r^2} = \langle r^2 \rangle = \langle r^{-2} \rangle = G_{r^{-2}}$ (5)
$G_{r^j s} = \langle r^j s \rangle$, $0 \le j \le 4$. (2) (orders).

- Orbit-Stabiliser Theorem

Let G act on a set X. For any $x \in X$, there is a bijection:

$\beta : G(x) \xrightarrow{1:1} \{ \text{left cosets w.r.t. } G_x \text{ in } G \}$.
$g(x) \longrightarrow gG_x$ [old notation: $\psi(g(x))$]

Proof: Preconsideration: string of equivalent statements, true for any $g, h \in G$.

For "fixed x", $g(x) = h(x) \overset{\text{"left multi" by } g^{-1}}{\Longleftrightarrow} g^{-1}(g(x)) = g^{-1}(h(x)) = g^{-1}g(x) = x$
$= g^{-1}h(x)$
$\overset{\text{defn}}{\Longleftrightarrow} g^{-1}h \in G_x \overset{G_x \text{ is a group}}{\Longleftrightarrow} g^{-1}hG_x = G_x \overset{\text{left multi by } g}{\Longleftrightarrow} hG_x = gG_x$

This gives (i) β is well defined.

[$g(x) = h(x)$ has to imply $gG_x = hG_x$, this is the "$\Rightarrow$" of the above preconsideration.].

(ii) β is injective

[If $\beta(g(x)) = \beta(h(x))$ has to imply $g(x) = h(x)$, this is "$\Leftarrow$" since

$gG_x \mapsto \beta(g(x)) = \beta(h(x)) = hG_x \Rightarrow g(x) = h(x)$]].

(iii) β is surjective.

[[Suppose C is a left coset of G_x. Need to find $\tilde{g} \in G$ s.t. $\beta(\tilde{g}(x)) = C$. but C must be of the form $\tilde{h}G_x$ for some $\tilde{h} \in G$ and $\beta(\tilde{h}(x)) = \tilde{h}G_x$, so put $g = \tilde{h}$]]. ∎

- Corollary: If G is finite, acting on a set X, then we have for any $x \in X$: $|G(x)|\,|G_x| = |G|$

[[In this sense, the size of the orbit of x is "complementary" to the size of the stabiliser of x.]].

Proof: Take orders (= sizes) in the O-S-T. $|G(x)| = |\{\text{left cosets of } G_x \text{ in } G\}|$.

Recall: all the cosets w.r.t. G_x have the same size $|G_x| = |eG_x| = |gG_x|$ $\forall g \in G$. Hence $|G|/|G_x|$ is the no. of cosets w.r.t. G_x by O-S-T $= |G(x)|$ ∎

Remember: the statement of the corollary is still valid for $|G| = \infty$, using standard conventions for multiplying cardinal numbers. ($n \cdot \infty = \infty$ $(n > 0)$, $\infty \cdot \infty = \infty$)

- Corollary: If the finite group G acts on a finite set X, then the orbit length divides the group order, i.e. $|G(x)|\,|G|$ $\forall x \in X$. In particular the size of any conjugacy class of G divides the group order. Some stabilisers are closely related:

- Prop^n: Suppose $X \in G(y)$ then G_x and G_y are conjugate to each other in G, i.e. $\exists\, h \in G$ s.t. $G_x = hG_yh^{-1}$.

Proof: As $x = h(y)$ for some $h \in G$, we find

$$G_x = \{g \in G \mid g(x) = x\} = \{g \in G \mid g(h(y)) = h(y)\}$$
$$= \{g \in G \mid \underbrace{h^{-1}(g(h(y)))}_{h^{-1}gh(y)} = h^{-1}(h(y)) = y\}$$
$$= \{g \in G \mid h^{-1}gh(y) = y\}$$

Now put $g' = h^{-1}gh$, then

$$= \{hg'h^{-1} \in G \mid g'(y) = y\} = h\{g' \in G \mid g'(y) = y\}h^{-1}$$

($\{g' \in G \mid g'(y) = y\} = G_y$)

Algebra lecture 30 continued

- Heading towards "Cauchy's Theorem".

p(prime) $| |G| \Rightarrow \exists$ subgroup $H < G$ with $|H| = p$.

[partial converse to Lagrange's Theorem].

Note: A_4 does not has a subgroup of order 6.

$|A_4| = 12$.

Algebra 04/03/2014

- Lecture 31

- Theorem (Cauchy)

Let G be a finite group, and p a prime dividing $|G|$. Then there is a subgroup G of order p.

Proof: Will use: orbit under the action of $\mathbb{Z}_p$ are of size 1 or p.

Main idea: Let $\mathbb{Z}_p$ act on a group related to G, more precisely on $\underbrace{G \times G \cdots \times G}_{p \text{ factors.}}$. The action is simply by

$$\mathbb{Z}_p \longrightarrow S_{G \times G \times \cdots G}$$

$$\bar{r} \longrightarrow \text{"shift cyclically by } r\text{" map "sh}_r\text{"}.$$

$$sh_r(g_1, \ldots g_p) = (g_{r+1}, g_{r+2}, \ldots g_p, g_1, g_2, \ldots g_{r-1}, g_r)$$

This clearly defines a bijection of $G \times \cdots \times G$ (the two sided inverse being sh_{p-r}).

Homomorphism property: $\bar{r} + \bar{s} \longrightarrow sh_s$ then sh_r

$$\overline{r+s} \longrightarrow sh_{r+s}.$$

Now consider a (slightly) smaller ~~(subgroup)~~ set

$$\Omega = \{(g_1, \ldots, g_p) \in G \times \cdots \times G \mid g_1 \cdots g_p = e_G\}$$

Claim1: The group action of $\mathbb{Z}_p$ on $G \times \cdots \times G$ restricts to one on Ω.

// To show: if $(g_1, \ldots g_p) \in \Omega$, then $(g_2, \ldots g_p, g_1) \in \Omega$. Then we're done since, by induction, any sh_r will ~~map~~ Ω to itself.

So let $(g_1, \ldots g_p) \in \Omega$, ie. $g_1 \cdots g_p = e_G \Rightarrow g_2 \cdots g_p = g_1^{-1}$.

$\Rightarrow g_2 \cdots g_p g_1 = g_1^{-1} g_1 = e_G \Rightarrow (g_2, g_3, \ldots g_p, g_1) \in \Omega$ //

Claim2: $|\Omega| = |G|^{p-1}$

// We can choose independently $g_1, \ldots, g_{p-1} \in G$ then g_p is uniquely determined as $g_p = (g_1 \cdots g_{p-1})^{-1} \Rightarrow$ have $|G|^{p-1}$ such // In particular, $p \mid |G| \mid |\Omega|$ ie. $p \mid |G|$ & $|G| \mid |\Omega|$.

Now we partition Ω into ~~orbits~~ orbits under the $\mathbb{Z}_p$-action ($\dot\cup$ = "disjoint union").

$$\Omega = \dot\cup \{\text{orbits of size } 1\} \dot\cup \dot\cup \{\text{orbits of size } p\}.$$

hence $|\Omega| = \sum_{\substack{\text{orbits of} \\ \text{size } 1}} 1 + \sum_{\substack{\text{orbits of} \\ \text{size } p}} p$, as $p \mid |\Omega|$ & $p \mid \sum_{\substack{\text{orbits} \\ \text{size } p}} p$

$\Rightarrow p \mid \#\{\text{orbits of size } 1\}$.

We know one of these: $\{e_G, e_G, \ldots e_G\}$ is an orbit.

There must be at least one (in fact $p-1$) more.
Claim: This must be of the form $(g,\dots,g)$ for some $g\in G, g\neq e_G$
This is an orbit of size 1 in Ω and $(g,\dots,g)$ satisfies $\underbrace{g\cdots g}_{g^p} = e_G$
$(g\neq e_G)$
$\Rightarrow g$ is of order p in G
(Ω doesn't have to be a subgroup of $G\times G\times\cdots G$). ∎
(↓ it is a set)

Theorem: Any group G of order $2p$, where p is a prime ≥ 3.
Then G is either cyclic or dihedral.
Proof: Use Cauchy's Theorem (twice):
(1) ∃ element in G of order 2, say a.
(2) ∃ element in G of order p, say b
It generates a group $B=\langle b\rangle$ of order p. Now $G\supsetneq B$ for any $g\in G\setminus B$
Claim: $a\in G\setminus B$.
[[Any element in B has order dividing p but a has order $2\Rightarrow$ can't be in B]].
Therefore $G = B\cup aB$
Where does ba lie? clearly $ba\notin B$
[[$ba=b^k \Rightarrow a=b^{k-1}\in B$ ⚡]].
hence must have $ba=ab^k$ for some k. $\Leftrightarrow$ $aba=b^k$ (as $a=a^{-1}$)
$ba=ab^k \Leftrightarrow b=ab^ka = (aba)^k = (b^k)^k = b^{k^2}$ (①)
$\Rightarrow p\mid (k^2-1)=(k+1)(k-1)$ [[b of order p]].
$\Rightarrow p\mid k-1$ or $p\mid k+1$ [[can choose $0\leq k\leq p-1$]].
Hence two possibilities:
$k=1 \Rightarrow ba=ab \Rightarrow$ abelian $\cong \langle a\rangle\times\langle b\rangle \cong \mathbb{Z}_2\times\mathbb{Z}_p \cong \mathbb{Z}_{2p}$ cyclic.
or $k=p-1 \to ba=ab^{-1}$ ie $aba=b^{-1}$.
the third relation for the dihedral group ($a\leftrightarrow s$, $b\leftrightarrow r$) ∎

「If a group has the size $2p$ (2 times) for our p a prime ≥ 3 (not less than).
Apply our sly trick to show that it's cyclic — or dihedral —
What else could it be?

Algebra 06/03/2014

-Lecture 32.

Conjugacy Classes for S_n and A_n

-Recall: For S_3 have conjugacy classes.

$\{e\}, \{(12),(23),(31)\}, \{(123),(321)\}$.

same "shape" (transp) same shape (3-cycles).

Instance of more general phenomenon.

-Def^n: Let $x \in S_n$, $x \neq e$; x can be written as a product of disjoint cycles $x=(a_1 \cdots a_{k_1})(b_1 \cdots b_{k_2}) \cdots (t_1 \cdots t_{k_r})$. ($r \geq 1$, $k_1 \leq k_2 \leq \cdots k_r$ of course $k_1 + \cdots + k_r \leq n$). Then we say that x has cycle shape $[k_1, \cdots k_r]$

-Example: $x=(12)(357)(894)$ has cycle shape $[2,3,3]$.

$x=(12)(357)(893)$ does not have cycle shape $[2,3,3]$; instead it has cycle shape $[2,5]$: $x=(12)(89357)$.

-Prop^n: Let $x=(i_1 \cdots i_k)$ be a k-cycle in S_n ($n \geq k$). Then for any $g \in S_n$, we can read off the action of g on x by conjugation as follows: $gxg^{-1}=(g(i_1) \cdots g(i_k))$

(view g as a bijection $\{1, \ldots n\}$ onto itself.)

-Example $x=(254) \in S_5$ $g=\begin{pmatrix}1&2&3&4&5\\2&3&5&1&4\end{pmatrix}$

Prop^n: $gxg^{-1}=(g(2)\ g(5)\ g(4))$

$=(3\ 4\ 1)$.

Compute $gxg^{-1}=(12354)(254)(45321)=(134)$.

Proof: Write $T=\{i_1, \ldots i_k\}$ the set of indices of x.

Case 1: $j \in T$, then $j=i_r$ for some $r \in \{1, \ldots k\}$.

and $gxg^{-1}(g(j)) = gxg^{-1}(g(i_r)) = gx(i_r) = \begin{cases} g(i_{r+1}) & \text{if } r<k \\ g(i_1) & \text{if } r=k \end{cases}$

($g(j) \in \{1 \ldots n\}$; $x(i_r) = i_{r+1}$)

Case 2: $j \notin T$ then $gxg^{-1}(g(j)) = gx(j) = g(j)$

Overall, gxg^{-1} is the bijection of $\{1, \ldots n\}$ given as cycle by $(g(i_1)\ g(i_2) \ldots g(i_k))$.

Put this together for (a product of) disjoint cycles.

- **Theorem:** For $x \in S_n$, the conjugacy class $CCl_{S_n}(x)$ consists of all the permutations of the same cycle shape.

Proof: Let $x = (a_1 \cdots a_{k_1})(b_1 \cdots b_{k_2}) \cdots (t_1 \cdots t_{k_r})$ be a product of disjoint cycles. Then $gxg^{-1} = g(a_1 \cdots a_{k_1})g^{-1}\, g(b_1 \cdots b_{k_2})g^{-1} \cdots g(t_1 \cdots t_{k_r})g^{-1}$.

$\overset{\text{by Prop}^2}{=} (g(a_1) \cdots g(a_{k_1}))(g(b_1) \cdots g(b_{k_2})) \cdots (g(t_1) \cdots g(t_{k_r}))$.

which has the same cycle shape as x since g is a bijection.

On the other hand, given x and $y \in S_n$ of the same cycle shape,

$x = (a_1 \cdots a_{k_1}) \cdots (t_1 \cdots t_{k_r})$

$y = (a_1' \cdots a_{k_1}') \cdots (t_1' \cdots t_{k_r}')$.

There is a bijection sending $a_1 \to a_1', \ldots, t_n \to t_n'$.

We can extend this to a bijection g of $\{1, \ldots n\}$. For such a g (not unique) we have $gxg^{-1} = y$. (use prop ^{n}). ∎

- **Example 1:** Conjugacy classes in S_4.

possible cycle shapes in S_4: ① [1] ② [2] [3] ④ [4] ③ [2,2]

$\{e\}$. $\{(12), (13), (14), (23), (24), (34)\}$.

For [3] ⑧: $\{(123), (132), (234), (243), (134), (143), (124), (142)\}$

$\{(1234), (4321), (1342), (2431), (1423), (3241)\}$.

For [2,2]: $\{(12)(34), (13)(42), (14)(23)\}$.

$1+6+8+6+3 = 24 \Rightarrow$ all the elements in S_4.

Example 2: S_6: [1], [2], [3], [4], [5], [6], [2,2], [2,3], [3,3], [2,2,2], [2,4].

In general, for S_n the cycle shapes are the non-decreasing partitions of n, where we drop the "1"s. ie. [1,1,2,2] = [2,2].

- Q: How many elements in each class?

Claim 1: For any m-cycle $x \in S_n$ have $|CCl_{S_n}(x)| = \frac{n(n-1)\cdots(n-m)}{m}$.

Claim 2: For cycle shape $[m_1, \ldots m_r]$, $m_1 \le \cdots \le m_r$.

then get $\gamma(n; m_1, \ldots m_r) = \frac{n(n-1)\cdots(n-m_1-1)}{m_1} \cdot \frac{(n-m_1)(n-m_1-1)\cdots(n-m_1+1-m_2)}{m_2} \cdots$

$\cdots \frac{(n-\sum_{i=1}^{r-1} m_i)(n-\sum_{i=1}^{r-1} m_i - 1)\cdots(n-\sum_{i=1}^{r} m_i + 1)}{m_r}$

Algebra

11/03/2014

- Lecture 33

- Example S_4: $[3]$ $[4]$ $[2,2]$

$\frac{4\cdot 3\cdot 2}{3}$ $\frac{4\cdot 3\cdot 2\cdot 1}{4}$ $\frac{\frac{4\cdot 3}{2}\cdot\frac{2\cdot 1}{2}}{2!}$ ← 6

(8) (6)

Recall: $H < S_n$ is normal $\Leftrightarrow$ H is $\cup$ {conj. classes}

- Formula: for # elts. in given conjugacy classes, for cycle shape

$[\underbrace{m_1,\dots m_1}_{s_1},\underbrace{m_2,\dots m_2}_{s_2},\dots,\underbrace{m_r,\dots m_r}_{s_r}]$ with $m_1<m_2<\dots<m_r$

$$\gamma(n,\underbrace{m_1,\dots m_1}_{s_1},\dots,\underbrace{m_r,\dots m_r}_{s_r}) = \left(\frac{n(n-1)\cdot\dots\cdot\left(n-\sum_{j=1}^{r}(m_j s_j+1)\right)}{\prod_{j=1}^{r} m_j^{s_j}}\right)\Big/(s_1!\cdots s_r!)$$

Example (1). For cycle shape $[2,2]$ in S_6 get $\frac{\frac{6\cdot 5}{2}\cdot\frac{4\cdot 3}{2}}{2!}$

(2) For $[2,2,2,3,3]$ in S_{12} get

$$\frac{\frac{12\cdot 11}{2}\,\frac{10\cdot 9}{2}\,\frac{8\cdot 7}{2}\,\frac{6\cdot 5\cdot 4}{3}\,\frac{3\cdot 2\cdot 1}{3}}{3!\cdot 2!} = \frac{12!}{12\cdot 6^2\cdot 2} = \dots$$

Normal subgroup H in S_n

- $H < S_n$ is normal $\Leftrightarrow$ H is a union of conjugacy classes.

Use that $|H|$ divides $|S_n|$]

- Example: $n=4$ S_4: cycle shapes.

cycle shape	$[1]$	$[2]$	$[3]$	$[4]$	$[2,2]$
# elements	1	$\frac{4\cdot 3}{2}$	$\frac{4\cdot 3\cdot 2}{3}$	$\frac{4\cdot 3\cdot 2\cdot 1}{4}$	$\frac{\frac{4\cdot 3}{2}\cdot\frac{2\cdot 1}{2}}{2!}$
	(1)	(6)	(8)	(6)	(3).

check: $\Sigma \#\{\text{conj. classes}\} = |S_4| = 1+6+8+6+3 = 24$.

for subgroups arising as a union of conjugacy classes. need to find linear combinations $1+\varepsilon_2\cdot 6+\varepsilon_3 8+\varepsilon_4 6+3\varepsilon_5$ dividing 24; $\varepsilon_i\in\{0,1\}$

Divisors of 24: (1), 2, 4, 3, 6, 8, 12, 24. (short hand for conjug. class characterized by this cycle shape)

2, 3 not possible, 4 is possible: $[1]\cup[2,2]$

6, 8 not possible, 12 is: $[1]\cup[2,2]\cup[3]$

Those indeed form subgroups! The first one $([1]\cup[2,2]) \cong$ Viktein-4 group. The second one give precisely the even elements in S_4 $\Rightarrow$ subgroup is A_4.

Conclusion: All the normal subgroups of S_4 are $\cong V$ or $\cong A_4$ (and $\{e\}, S_4$).

Conjugacy Classes in A_n

- $A_n \subset S_n$, recall $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$. If $x \in A_n$, clearly $ccl_{A_n}(x) \subseteq ccl_{S_n}(x)$. Now both cases $\subsetneq$ and $=$ occur!

- Example (1): "$\subsetneq$" $n=3$ $x \in (1\,2\,3)$.
$ccl_{S_3}(x) = \{(1\,2\,3), (3\,2\,1)\}$. but A_3 is abelian ($\cong \mathbb{Z}_3$) as 3 is prime hence all conjugacy classes have size 1 $\Rightarrow ccl_{A_3}(x) = \{(1\,2\,3)\} \neq ccl_{S_3}(x)$.

(2) "$=$": $n=5$. $x \in (1\,2\,3) \Rightarrow ccl_{S_5}(x) = \{$all 3-cycles in $S_5\}$.
Since x commutes with an odd $\sigma \in S_5$, the following proposition guarantees that $ccl_{A_5}(x) = ccl_{S_5}(x)$. (take $\sigma = (4\,5)$).

- Prop^n: Let $x \in A_n$ $(n \geq 2)$ (i) If x commutes with some odd permutation in S_n, then $ccl_{A_n}(x) = ccl_{S_n}(x)$

(2) If x does not commute with any odd permutation in S_n then $ccl_{S_n}(x) = ccl_{A_n}(x) \dot\cup ccl_{A_n}((1\,2)x(1\,2)^{-1})$ ($\dot\cup$ disjoint union)
ie. the conjugacy class of x in S_n splits into 2 conj. classes in A_n of equal size with representatives x and $(1\,2)x(1\,2)^{-1}$

Proof: (i) Suppose x commutes with some $g \in S_n$, g odd.
(ie $xg = gx \Leftrightarrow gxg^{-1} = x$).
Then take $y \in ccl_{S_n}(x)$ ie. $y = hxh^{-1}$ for some $h \in S_n$.
To show ~~y is also $\in$~~ $y \in ccl_{A_n}(x)$.
Clearly either h or hg is an odd permutation, and both conjugate x into y. (for h clear by def^n).
for hg: $(hg)x(hg)^{-1} = h(gxg^{-1})h^{-1} = hxh^{-1} = y$.
conclusion: $ccl_{A_n}(x) = ccl_{S_n}(x)$.

(ii) Assume that x does not commute with any odd permutation in S_n
Then the stabilizer $(S_n)_x$ is the same as in A_n:
$(S_n)_x = \{g \in G \mid gxg^{-1} = x\}$. (*) (where $G = S_n$).
but by assumption, no odd permutation contributes, so (*) $= \{g \in G \mid g$ even, $gxg^{-1} = x\} = \{g \in A_n \mid gxg^{-1} = x\} = (A_n)_x$.
Corollary to Orbit-Stabilizer Theorem gives

$$|ccl_{A_n}(x)| = \frac{|A_n|}{|(A_n)_x|} = \frac{\frac{1}{2}|S_n|}{|(S_n)_x|} = \frac{1}{2}|ccl_{S_n}(x)|$$

Algebra lecture 33 continued.

Now note that every odd permutation in S_n is of the form $(12)g$, $g \in A_n$. $ccl_{A_n}((12)x(12)^{-1}) = \{hxh^{-1} \mid h \in S_n, \text{odd}\}$.

[[Clear bijection

$$ccl_{A_n}(x) \leftrightarrow ccl_{A_n}((12)x(12)^{-1})$$]].

So the conjugacy class of $x \in S_n$ break up as follows

$$ccl_{S_n}(x) = ccl_{A_n}(x) \cup ccl_{A_n}((12)x(12)^{-1})$$ ∎.

Algebra 13/03/2014

-Lecture 34

-Determine the cycle shapes for S_n, then decide, for each such conjugacy classes for even permutations, if it splits (into 2 classes of equal size) in A_n.

-Criterion: The class (of an even $x \in S_n$) splits into two such in A_n iff x does not commute with any odd permutations in S_n.

Example 1. A_4, first look at the cycle shapes in S_4.

S_4	[1]	[2]	[3]	[4]	[2,2]
ev/od	ev	od	ev	od	ev
in A_4?	✓	✗	✓	✗	✓
# elements	(1)	(6)	(8)	(6)	(3)

The first one and last one clearly do not split into two subsets of equal size, as their size is odd. The middle one does split. Take any representative, say $x=(1\,2\,3)$, and suppose $g \in S_4$ satisfies $gx=xg$ i.e. $gxg^{-1}=x$.

Recall $g(1\,2\,3\,4)g^{-1}=(g(1)\ g(2)\ g(3))$.

Q: When is $(g(1)\ g(2)\ g(3))=(1\,2\,3)=(2\,3\,1)=(3\,1\,2)$.

Possibilities. $g(1)=1$ 2 3

$g(2)=2$ 3 1

$g(3)=3$ 1 2.

Necessarily: $g(4)=4$ in all these cases $\Rightarrow$ corresponding bijections are e, $(1\,2\,3)$ or $(1\,3\,2)$, but these are all even $\xrightarrow{\text{criterion}}$ [3] splits into $ccl_{A_4}(x)$ ($=(1\,2\,3)$) and $ccl_{A_4}(\underbrace{(1\,1\,2)x(1\,2^{-1})}_{(1\,2\,3)=(1\,2\,3)})$

-Example 2 (revisited): The class of $x=(1\,2\,3)$ in S_n ($n \geq 5$). does not splits as it commutes eg. with $(4\,5)$, an odd permutation.

-Example 3: The class of $x=(1\,2\,3\,4)(5\,6\,7\,8\,9\,10)$ does not split in S_{10} as it commutes with $(1\,2\,3\,4)$ an odd permutation

- Normal subgroups of A_n (similar procedure to the one for S_n) in fact easier as there are fewer conjugacy classes.

Example: A_4. only one non-trivial normal subgroup.
A_n, $n \geq 5$: no normal subgroups.

Classification of Finite Groups of Order p^2 (p prime)

- Recall: Properties of centre.
(1) $Z(G)$ = union of all conjugacy classes of size 1.
(2) $Z(G)$ is normal in G.
(3) $Z(G) = G \Leftrightarrow G$ is abelian.
(4) Let G act on itself by conjugation. Then $Z(G) \subset G_h$ for any $h \in G$

- Prop^n: Let p be a prime and G a group of order p^r, ($r \geq 1$). Then the centre is non-trivial.

Proof: Argument similar to the one in Cauchy's Theorem, G is the union of disjoint conjugacy classes. $\overset{\text{enumerate}}{\Rightarrow} |G| = \sum_x |ccl_G(x)|$ (**)
(Sum over set of representatives of ccl's)
Use: size of any conj. class divides $|G| = p^r$, so is of the form p^i, $i \in \{0, \dots, r\}$. (*)
Suppose, for a contradiction, $Z(G) = \{e\}$. Then by property (1) above, there is no other ccl. of size 1, hence by (*) is of size p^i, $i \geq 1$, in particular divides by p.
But then $p \mid$ LHS (**) but not the RHS.
Conclusion: $Z(G) \neq \{e\}$.
RHS of (**), possible sizes of conjugacy classes are $1, p, \dots p^r$.
$\Rightarrow$ count RHS of (**) as $a_0 \cdot 1 + a_1 p + \dots + a_r p^r$ with $a_0 = 1$ and $a_i \geq 0 \in \mathbb{Z}$.
mod p this gives 1.

- Corollary: Let p be a prime and G of order p^2. Then G is abelian.

Proof: From the prop^n above we get $Z(G) \neq \{e\}$.
Case 1: $\exists$ element of order p^2 in G, but then G is cyclic, in particular, abelian $\lightning$ ✓

Algebra lecture 34 continued.

Case 2: No element in G has order p^2, then any other element (#e) in G has order p.

(i) $|Z(G)| = p^2 \Rightarrow Z(G) = G$.

as $G \supset Z(G)$ as a subgroup and has the same size.

(ii) Assume $|Z(G)| = p$, then $\exists\, h \in G \setminus Z(G)$, in particular $|cl_G(h)| > 1$ (property (1)) for $Z(G)$ above. By property (4), $Z(G) \subset G_h$, so. $Z(G) \leq G_h$. O-S-T gives $|cl_G(h)| \cdot |G_h| = |G|$

$\geq p \quad \geq p \quad = p^2$.

$\Rightarrow |cl_G(h)| = p = |G_h|$.

and in particular $Z(G) = G_h$ ($G_h \supset Z(G)$, same size).

know $h \in G_h$.

Conclusion: (#ii) cannot hold $\Rightarrow$ G abelian

— Theorem (classification of groups of order p^2)

$|G| = p^2 \Rightarrow G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Algebra 18/03/2014.

- Lecture 35.

Classification of finitely generated abelian groups.

- So far: classification results for groups of order $2p$ and p^2, p prime. Larger class, all abelian groups. ("finitely generated")

- Recall: G is finitely generated if $\exists$ finite set $\{g_1, \dots g_n\}$ st. any element is expressed in terms of the g_i and their inverses.

Example:
- $D_n = \langle r, s | \dots \rangle$ is generated by 2 elements.
- Any finite group is obviously finitely generated.
- $(\{2^a | a \in \mathbb{Z}\}, \cdot)$ is generated by $\{2\}$.
- $(\{2^a \cdot 17^b \cdot 31^c | a,b,c \in \mathbb{Z}\}, \cdot)$ is gen. by $\{2, 17, 31\}$.
- $(\mathbb{Z}, +)$ is generated by $\{1\}$.
- $\mathbb{Z} \times \mathbb{Z}_5 \times \mathbb{Z}$ is gen. by $\{(0, \bar{0}, 1), (0, \bar{1}, 0), (1, \bar{0}, 0)\}$.

Non-example: $(\mathbb{Q}, +)$ is not finitely generated.
[Suppose $\{\frac{p_1}{q_1}, \dots \frac{p_r}{q_r}\}$ is a set of generators for $\mathbb{Q}$. Then any element would be of the form $a_1 \frac{p_1}{q_1} + \dots + a_r \frac{p_r}{q_r}$ for some $a_i \in \mathbb{Z}$ hence would have bounded denominator. ⚠]

From now on, consider only abelian groups, will (hence) write them in additive notation. Moreover, any G will be finitely generated (f.g.) ie. $G = \langle g_1, \dots g_n \rangle$ for some $g_i \in G = \{a_1 g_1 + \dots + a_n g_n | a_i \in \mathbb{Z}\}$

Note: Some of these $(a_i g_i)$ might coincide (there might be relations among generators).

Example: $\mathbb{Z} = \langle 2, 3 \rangle = \{a_1 \cdot 2 + a_2 \cdot 3 | a_1, a_2 \in \mathbb{Z}\}$ (Here a relation is given for $(a_1, a_2) = (3, -2)$)

Actually, we can get G (f.g. abelian) as a quotient of some $\mathbb{Z}^M$ for some $M \in \mathbb{N}$. In fact we can choose $M = n$ where $G = \langle g_1, \dots, g_n \rangle$. Define a group homomorphism

$$\varphi : \mathbb{Z}^n \to G$$

$$a = (a_1, \dots a_n) \longmapsto a_1 g_1 + \dots + a_n g_n.$$

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) \quad a_1, a_2 \in \mathbb{Z}^n.$$

Clearly φ is surjective.

- **Theorem:** Any f.g. abelian group G is isomorphic to the quotient of some $\mathbb{Z}^M$ (for some $M \geq 1$). More precisely, if G is generated by $\{g_1, \dots g_n\}$ then we have

$$\boxed{G \cong \mathbb{Z}^n / k \text{ for some } k \leq \mathbb{Z}^n}$$

Proof: Invoke first isomorphism theorem for groups, $k = \ker(\varphi)$, φ as above.

- **Example (Revisited):** $G = \mathbb{Z} = \langle 2, 3 \rangle$.

$\Rightarrow G = \mathbb{Z}^2 / k$, $k = \langle \underbrace{(3, -2)}_{\in \mathbb{Z}^2} \rangle \cong \mathbb{Z}$. $\leq \mathbb{Z}^2$

- **Def^n:** (i) In the situation of Theorem above, we call k the ~~relat~~ relations subgroup of G.

(ii) Suppose there are no non-trival relations among the g_i (i.e. $\sum_{i=1}^{n} a_i g_i = 0 \Rightarrow a_i = 0$) then we call $\{g_1, \dots g_n\}$ a free generating set. and G a free abelian group of rank n.

Typical example: $\mathbb{Z}^r$ is a free abelian group of rank r.

- **Prop^n:** Every subgroup of $\mathbb{Z}^n$ is itself f.g. and free of rank $\leq n$.

Proof (idea): By induction.

Clear for $n = 1$: any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. For $n > 1$, reduce $k \leq \mathbb{Z}^n$ to smaller rank by "projecting onto last factor", i.e. $\pi : k \longrightarrow \mathbb{Z}$

$$(a_1, \dots a_n) \longmapsto a_n$$

If $\pi(k) = \{0\}$, then $k \leq \underbrace{\mathbb{Z}^{n-1} \times \{0\}}_{\leq \mathbb{Z}^n} \cong \mathbb{Z}^{n-1}$ so induction applies.

Otherwise there is a smallest possible integer $b \in \pi(k)$ and $\pi(k) = \langle b \rangle \cong \mathbb{Z}$.

Then use criterion for direct products for proving that

$k \cong k_0 \times \langle b \rangle$ where $k_0 = \{a \in k \mid a_n = 0\}$

and induction applies $\subseteq \mathbb{Z}^{n-1} \times \{0\} \cong \mathbb{Z}^{n-1}$.

- Remember: by above prop^n, any $k \leq \mathbb{Z}^n$ is of the form $k = \langle \underline{a}_1, \dots \underline{a}_m \rangle$ for $\underline{a}_i \in \mathbb{Z}^n$. From this we can form a matrix $A = A(k)$ $A = \begin{pmatrix} \underline{a}_1 \\ \vdots \\ \underline{a}_m \end{pmatrix}$, an $m \times n$ matrix with integer entries. (Linear Algebra, vector space homomorphisms).

Algebra lecture 35 continued

A describes a group homomorphism $\mathbb{Z}^m \to \mathbb{Z}^n$ whose image is given by K.

$x \longrightarrow A^t x$, integer entries

— Def^n: If $G \cong \mathbb{Z}^n/K$ and $A = A(K)$ as in the above remark, then we call A a relation matrix for G.

As in linear Algebra can choose many different (but equivalent) ways to obtain such a relation matrix.

Ambiguity: can multiply by any $\gamma \in GL_m(\mathbb{Z})$ on the left by any $\delta \in GL_n(\mathbb{Z})$ on the right.

Elementary row/column operation ↘

Aim: find a "normal form" for a relation matrix. ie. given $A \in M_{m\times n}(\mathbb{Z})$ find $\tilde{A}$ in "diagonal form" which is equivalent to A, ie.

$\tilde{A} = PAQ$, $P \in GL_m(\mathbb{Z})$, $Q \in GL_n(\mathbb{Z})$.

Allowed "moves": (very similar to Gauss-Jordan elimination, but with an important difference.

① Add an integer multiple of some row/column to another row/column.

② Swap two rows/columns

③ multiply a row/column by ± 1.

Claim: There is an algorithm which allows to pass from $A \in M_{m\times n}(\mathbb{Z})$ to one where only the diagonal entries are "possibly" non-zero.

Algebra 20/03/2014

-Lecture 36.

-Typical setting:

$$A=\begin{pmatrix}8&-4&22\\4&-8&8\end{pmatrix} \xrightarrow{r_1\leftrightarrow r_2} \begin{pmatrix}4&-8&8\\8&-4&22\end{pmatrix} \xrightarrow{r_2\to r_2-2r_1} \begin{pmatrix}4&-8&8\\0&12&6\end{pmatrix}$$

$$\xrightarrow{C_2\to C_2+2C_1} \begin{pmatrix}4&0&8\\0&12&6\end{pmatrix} \xrightarrow{C_3\to C_3-2C_1} \begin{pmatrix}4&0&0\\0&12&6\end{pmatrix} \xrightarrow{C_2\to C_2-2C_3} \begin{pmatrix}4&0&0\\0&0&6\end{pmatrix}$$

$$\xrightarrow{C_2\leftrightarrow C_3} \begin{pmatrix}4&0&0\\0&6&0\end{pmatrix}$$

Now add zeros to make it a square matrix $\to \begin{pmatrix}4&0&0\\0&6&0\\0&0&0\end{pmatrix}$

Claim: We can find a diagonal form s.t. ~~$a_{1,1}|a_{2,2}|\dots$~~ $a_{i,i}\mid a_{i+1,i+1}$ for any i.

In the example, we go further: $\begin{pmatrix}4&0&0\\0&6&0\end{pmatrix} \xrightarrow{r_1\to r_1+r_2} \begin{pmatrix}4&6&0\\0&6&0\end{pmatrix}$.

$$\xrightarrow{C_1\leftrightarrow C_2-C_1} \begin{pmatrix}4&2&0\\0&6&0\end{pmatrix} \xrightarrow{C_1\leftrightarrow C_2} \begin{pmatrix}2&4&0\\6&0&0\end{pmatrix} \xrightarrow{r_2\to r_2-3r_1} \begin{pmatrix}2&4&0\\0&-12&0\end{pmatrix}$$

$$\xrightarrow{r_2\to -r_2} \begin{pmatrix}2&4&0\\0&12&0\end{pmatrix} \xrightarrow{C_2\to C_2-2C_1} \begin{pmatrix}2&0&0\\0&12&0\end{pmatrix}.$$

Then add row of zeros ($\to$ square matrix), then indeed $a_{11}\mid a_{22}\mid a_{33}=0$

-Example: Let G be the group generated by $n=3$ generators x,y,z subject to the following relations:

$$8x-4y+22z=0$$
$$4x-8y+8z=0$$

Find a product of cyclic groups to which G is isomorphic.

Sol^n: To solve this, write $G=\mathbb{Z}^3/K$, where $K=\langle(8,-4,22),(4,-8,8)\rangle$ with the relation matrix $A=A(K)$ as above. From the completed (square) matrix we can read off the structure of G:

$$\begin{pmatrix}4&&\\&6&\\&&0\end{pmatrix} \xrightarrow{\text{read off}} G=\underbrace{\mathbb{Z}/4}_{\mathbb{Z}_4}\times\underbrace{\mathbb{Z}/6}_{\mathbb{Z}_6}\times\underbrace{\mathbb{Z}/0}_{\mathbb{Z}}, \text{ or also from } \begin{pmatrix}2&0&0\\0&12&0\end{pmatrix} \text{ get } G\cong\mathbb{Z}_2\times\mathbb{Z}_{12}\times\mathbb{Z}_0$$

The above is an example of the following classification theorem.

-Theorem (Fundamental Theorem of finitely generated abelian groups, (FTFGAG)): Let G be a finitely generated abelian group. Then G is

Isomorphic to a group of the following form:

$$\boxed{\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^r} \quad \text{with } r \geq 0,\ k \geq 0,\ d_j \geq 0.$$

Moreover, it is unique if we demand $d_1 | d_2 | \cdots | d_k$, $d_i > 1$.

- Defn: The number r as in the theorem is called the rank of G, and the $d_1, \ldots d_k$ with the condition $d_1 | d_2 | \cdots | d_k$ are the torsion invariants of G ($d_i > 1$).

Remember:

(1) G is finite $\Leftrightarrow r = 0$.

(2) The conditions $r = k = 0$ gives the trivial group.

(3) Whenever we have an entry $= \pm 1$" in the relation matrix, the we can ignore the corresponding factor in the direct product of the cyclic factors, since $\mathbb{Z}/1\mathbb{Z} \cong \{e\}$.

In particular, "1" never occurs as a torsion invariant.

(4) The torsion invariant have to be given with repetitions (multiplicities) ie. $\mathbb{Z} \times \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{105}$ has torsion invariants

$$\underbrace{7, 7}_{\text{twice}}, 105 \quad (\text{no "1"s!}).$$

- Application: Classify all the abelian groups of a given order.

Example: Classify all abelian groups of order $200 (= 2^3 \cdot 5^2)$.

The only primes involved are 2, 5.

To find: All possibilities of writing $d_1 \cdots d_k$ s.t. $1 < d_1 | d_2 | \cdots | d_k$ and $d_1 \cdot d_2 \cdots d_k = 200$.

The condition $d_1 | d_2$ translates into

exponent of 2 in $d_1 \leq$ exponent of 2 in d_2.

exponent of 5 in $d_1 \leq$ exponent of 5 in d_2.

Need to find all:

(1) Non-decreasing partitions of 3 (max power of 2 dividing gp order)

(2) Similar for 5

Overall, get 3×2 different possibilities (independent events).

Non-decreasing part. of 3 are 1, 1, 1 , 1, 2 and 3.

Non-decreasing parts of 2 are 1, 1 and 2.

36. Algebra lecture 36 continued

Get the following scheme

exponent of 2	1,1,1	1,1,1	1,2	1,2	0,3	3
exponent of 5	0,1,1	0,0,2	1,1	0,2	1,1	2
$d_1, \dots, d_k$	$2^1 5^0, 2^1 5^1, 2^1 5^1$	$2^1, 2^1, 2^1 5^2$	$2^1 5, 2^2 5$	$2, 5^2 2^2$	$5, 2^3 5$	$2^3 \cdot 5^2$
resulting gp.	$\mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{10}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{50}$	$\mathbb{Z}_{10} \times \mathbb{Z}_{20}$	$\mathbb{Z}_2 \times \mathbb{Z}_{100}$	$\mathbb{Z}_5 \times \mathbb{Z}_{40}$	$\mathbb{Z}_{2^3} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_{2^3 \cdot 5^2}$ $= \mathbb{Z}_{200} \times \mathbb{Z}_{200}$

- Defn: Let G be finite. Then $A_m(G) = |\{g \in G \mid mg = 0\}| = |\{g \in G \mid$ order of g divides $m\}|$.

  $O_m(G) = |\{g \in G \mid mg = 0$ and $kg \neq 0$ for $0 < k < m\}|$.
  $= |\{g \in G \mid$ order $= m\}|$

  Exercise: A_m is multiplicative: $A_m(G \times H) = A_m(G) \times A_m(H)$.

- Propn: $A_m(\mathbb{Z}_n) = \gcd(m,n)$.

  $O_{p^r}(G) = A_{p^r}(G) - A_{p^{r-1}}(G)$.

- Example: elements of order 8 in $\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}$ are $\gcd(8,12) \cdot \gcd(8,40) \cdot \gcd(8,102) = 64$.