Lecture 11

Repetition: Symmetric group S_n = "all permutations of $\{1,2,3,\dots,n\}$"

Every group is isomorphic to a subgroup of some S_n.

New notation: $\begin{pmatrix}1&2&3&4&5\\1&3&5&4&2\end{pmatrix} \in S_5$ can be written

as $2 \to 3 \to 5$ (we omit $1 \to 1$, $4 \to 4$),

or preferably as $(2\ 3\ 5)$

Note: $(2\ 3\ 5) = (5\ 2\ 3) = (3\ 5\ 2)$

Note: $(1\ 2\ 3) = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ in S_3, but

$(1\ 2\ 3) = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$ in S_4.

Def: $(2\ 3\ 5)$ is a 3-cycle.

Ex: Identity perm. in S_3: (1), (2) or (3).

Composition: $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \circ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

becomes $(1\ 2)(2\ 3) = (1\ 2\ 3)$ (the arrows illustrate $\underline{3} \to 2 \to \underline{1}$)

Def: Two cycles are disjoint if they have no common

elements (ex., $(1\ 3)$ and $(2\ 5\ 4)$).

For example $(1\ 2)(2\ 3) \neq (2\ 3)(1\ 2)$, but

Theorem: Two disjoint cycles commute.

Proof: Exercise.

Not every permutation is one cycle:

$\sigma = \begin{pmatrix}1&2&3&4&5&6&7\\5&1&7&2&4&6&3\end{pmatrix}$. Start with 1:

$(1\ 5\ 4\ 2)$, continue with 3: $(3\ 7)$, $6 \to 6$, so

we have $\sigma = (1\ 5\ 4\ 2)(3\ 7)$.

Theorem: Every permutation is a product of disjoint cycles.

Proof: Same principle as above.

Def: transposition = 2-cycle

Corollary: Every permutation is a product of transpositions.

Proof: We only need to consider cycles, and

$(a_1\ a_2\ a_3 \cdots a_k) = (a_1\ a_k)(a_1\ a_{k-1}) \cdots (a_1\ a_3)(a_1\ a_2)$

$\square$

Ex: $(1) = (1\ 2)(1\ 2) = (1\ 2)(3\ 4)(1\ 2)(3\ 4)$

$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3)$,

so product, or number, of transpositions is not unique.

Def: Permutation is called odd if it can be written as a product of an odd number of transpositions, and even if product of even number.

Theorem: No permutation is both odd and even.

Lemma: The identity permutation is not odd.

Proof (lemma): By contradiction: assume $(1) = \tau_k \tau_{k-1} \cdots \tau_2 \tau_1$, τ_i transp., k odd. For c in some τ_i, let τ_r be the first from right containing c; $\tau_r = (c\ d)$.

We know that $r \neq k$, since $(1) = (c\ d) \underbrace{\tau_{k-1} \cdots \tau_1}_{\text{no } c}$, gives $c \to d$, contradiction.

Possibilities for τ_{r+1}: I) $(x\ y)$ where $x, y \neq c, d$

II) $(x\ d)$

III) $(c\ y)$

IV) $(c\ d)$

I) $(x\ y)(c\ d) = (c\ d)(x\ y)$ (disjoint)

II) $(x\ d)(c\ d) = (c\ x)(x\ d)$

III) $(c\ y)(c\ d) = (c\ d)(d\ y)$,

so for case I–III we can move c one step to the left, i.e. increase r by one. Since $r \neq k$, we will end up with case IV: $(c\ d)(c\ d)$, but this is $= (1)$ and can be cancelled $\Rightarrow (1) = \sigma_{k-2} \cdots \sigma_2 \sigma_1$.

Same procedure with new c:s will eventually give $(1) = (a\ b)$ (since k odd), a contradiction. $\square$

Proof (theorem): Assume $\alpha = \sigma_1 \cdots \sigma_k = \tau_1 \cdots \tau_r$, k odd, r even. Then

$(1) = \alpha\alpha^{-1} = \sigma_1 \cdots \sigma_k \tau_r^{-1} \cdots \tau_1^{-1}$, $k + r$ odd,

a contradiction. $\square$

Def: All even permutations of S_n is called the alternating group A_n. (Exercise: check that A_n group!)

Theorem: A_n normal in S_n, and $|A_n| = \frac{n!}{2}$.

Proof: Define $f: S_n \to \mathbb{Z}_2$ by $f(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ even} \\ 1 & \text{if } \sigma \text{ odd} \end{cases}$

Check that f well-def. surj. hom. with kernel A_n

$\Rightarrow A_n$ normal and $S_n/A_n \cong \mathbb{Z}_2$

$$\Rightarrow \quad 2 = |\mathbb{Z}_2| = \left|S_n/A_n\right| = \frac{|S_n|}{|A_n|} = \frac{n!}{|A_n|} \Rightarrow |A_n| = \frac{n!}{2}. \ \square$$

Note: Chapter 7.10 (not in the course) is devoted to prove that $n \neq 4 \Rightarrow A_n$ simple.

Chapter 10 (10.1):

F field, V abelian group (written additively), scalar multiplication $F \times V \to V : (a,v) \mapsto av$.

Def: V is a vector space over F if for all $a_1, a_2 \in F$, $v_1, v_2 \in V$:

(i) $a_1(v_1+v_2) = a_1v_1 + a_1v_2$

(ii) $(a_1+a_2)v_1 = a_1v_1 + a_2v_1$

(iii) $a_1(a_2v_1) = (a_1a_2)v_1$

(iv) $1_F \cdot v_1 = v_1$

Ex: $\mathbb{R}^3$ vector space over $\mathbb{R}$

Ex: $F[x]$ vector space over F

Ex: $\mathbb{C}$ vector space over $\mathbb{R}$, but $\mathbb{R}$ not vector space over $\mathbb{C}$

More generally, K extension field of F $(K \supseteq F)$

$\Rightarrow$ K vector space over F (usual add. and mult.)

Def: w linear combination of $v_1, v_2, \ldots, v_n$ if

$w = a_1v_1 + a_2v_2 + \cdots + a_nv_n, \quad w, v_1, \ldots, v_n \in V, \ a_1, \ldots, a_n \in F.$

If every $w \in V$ is a lin. comb. of $v_1, \ldots, v_n$ then $\{v_1, v_2, \ldots, v_n\}$ spans V (over F).

Ex: $\{(1,0,0), (0,1,0), (0,0,1), (2,3,4)\}$ spans $\mathbb{R}^3$, $(2,3,4)$ lin. comb. of $(1,0,0), (0,1,0), (0,0,1)$.

Def: $\{v_1, v_2, \ldots, v_n\}$ linearly independent (over F) if $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0_V \Rightarrow a_i = 0_F$ for all i.

Def: $\{v_1, v_2, \ldots, v_n\} \subseteq V$ is a basis of V if

① it spans V and ② it is linearly independent

> **Lemma:** $\left.\begin{array}{l}\{v_1, v_2, \ldots, v_n\} \text{ spans } V \\ \{u_1, u_2, \ldots, u_m\} \text{ lin. indep}\end{array}\right\} \Rightarrow m \leq n$

Proof: See book

> **Theorem:** Any two bases of V over F have the same number of elements.

Proof: Assume $\{v_1, v_2, \ldots, v_n\}$ and $\{u_1, u_2, \ldots, u_m\}$ bases.

v_i spans V, u_j lin. indep. $\Rightarrow m \leq n$ by lemma

u_j span V, v_i lin. indep. $\Rightarrow n \leq m$, so $m = n$. $\square$

Def: The dimension of V over F, $[V:F]$, is the number of elements in any basis.

Ex: $F[x]$ infinite-dimensional over F, basis for example $\{1, x, x^2, \ldots\}$.

Ex: $p(x)$ irr. of degree $n \Rightarrow$ any element of $F[x]/(p(x))$ can be written $a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ (uniquely) $\Rightarrow \left[F[x]/(p(x)) : F\right] = n$.

Ex: $[\mathbb{C}:\mathbb{R}] = 2$, basis $\{1, i\}$ $\left(\mathbb{C} \simeq \mathbb{R}[x]/(x^2+1)\right)$

F, K, L fields, $F \subseteq K \subseteq L$.

> **Theorem:** If $[L:K]$ and $[K:F]$ are finite, then
> $$[L:F] = [L:K][K:F].$$

Proof: Assume $[L:K] = n$, basis $v_1, v_2, \ldots, v_n$

$[K:F] = m$, basis $u_1, u_2, \ldots, u_m$

Claim: all u_jv_i, $\begin{array}{l}1 \leq i \leq n \\ 1 \leq j \leq m\end{array}$, basis for L over F.

Spans: For $w \in L$: $w = b_1v_1 + b_2v_2 + \cdots + b_nv_n$, $b_i \in K$

For each b_i: $b_i = a_{1i}u_1 + a_{2i}u_2 + \cdots + a_{mi}u_m$, $a_{ji} \in F$

$$\Rightarrow w = \sum_i b_iv_i = \sum_i \Big(\sum_j a_{ji}u_j\Big)v_i = \sum_{i,j} a_{ji}u_jv_i.$$

Lin. indep.: $$\sum_{i,j} c_{ji}u_jv_i = \sum_i \Big(\sum_j c_{ji}u_j\Big)v_i = 0$$

$\Rightarrow$ all $\sum_j c_{ji}u_j = 0$ (v_i's lin. indep)

$\Rightarrow$ all $c_{ji} = 0$ (u_j's lin. indep.)

All u_jv_i basis $\Rightarrow [L:F] = mn$. $\square$

> **Theorem:** K, L finite-dim. extension fields of F, $f: K \to L$ isom. with $f(c) = c$ for all $c \in F$. Then $[K:F] = [L:F]$.

Proof: If $[K:F] = n$ with basis $\{u_1, u_2, \ldots, u_n\}$, show that $\{f(u_1), f(u_2), \ldots, f(u_n)\}$ is basis for L over F $\Rightarrow [L:F] = n$. $\square$