MATH 417

9/5/2018
We

4.1

Last time Let X be a set.

A permutation $\sigma \in Sym(X)$ is a cycle of length r if there exist $x_1, \dots x_r \in X$, all distinct, so that

$\sigma(x_1) = x_2$, $\sigma(x_2) = x_3$ $\dots$ $\sigma(x_r) = x_1$

and $\sigma(x) = x$ for $x \neq x_1, \dots x_r$.

Two permutations $\sigma, \tau \in Sym(X)$ are disjoint if for any $x \in X$ (if $\sigma(x) \neq x$ then $\tau(x) = x$) and (if $\tau(x) \neq x$ then $\sigma(x) = x$)

Remark It may happen that $\tau(x) = x = \sigma(x)$ for some $x \in X$.

What's not allowed is: ($\tau(x) \neq x$ and $\sigma(x) \neq x$).

We proved:

Lemma 3.1 If $\sigma, \tau \in Sym(X)$ are disjoint then

$$\sigma \circ \tau = \tau \circ \sigma.$$

Thm 3.2 Any $\sigma \in Sym(X)$, X a finite set, can be written uniquely (up to order) as a product (ie composition) of disjoint cycles

(same as Goodman, 1.5.3).

Proof 1. (existence of the decomposition). Induction on $|X|$.

- If $|X| = 1$, $Sym(X) = \{id_X\}$, so true.
- Suppose for any set Y with $|Y| \leq n$ any $\tau \in Sym(Y)$ can be written as a product of disjoint cycles, $|X| = n+1$ and $\pi \in Sym(X)$. If $\pi = id_X$, nothing to prove.

Suppose $\pi \neq id_X$. Then $\exists x_0 \in X$ s.t. $x_1 = \pi(x_0) \neq x_0$.

Now let $x_2 = \pi(x_1)$, $x_3 = \pi(x_2)$, $\dots$, $x_i = \pi(x_{i-1})$ $\dots$

Since X is finite not all x_i's are distinct.

Let k = largest integer so that $x_0, \dots, x_k$ are all distinct.

Claim $\pi(x_k) = x_0$.

Aside Recall: $f: A \to B$ is 1–1 if $\forall\, b \in B$ the equation $b = f(x)$ has at most one solution.

[Thus if $f(x_1) = f(x_2)$, we must have $x_1 = x_2$]

Proof of claim. Since k is the largest integer so that $x_0, \dots x_k$ are distinct, $x_0, \dots x_k, x_{k+1} = \pi(x_k)$ are not all distinct. So $x_{k+1} = x_i$ for some i, $0 \le i \le k$.

If $x_{k+1} \neq x_0$, then $x_{k+1} = x_i$ for some $i > 0$. $\Rightarrow$

$$\pi(x_k) = x_{k+1} = x_i = \pi(x_{i-1})$$

But π is 1–1. $\Rightarrow$ $x_k = x_{i-1}$ and $0 \le i-1 < k$

This contradicts that $x_0, \dots x_k$ are all distinct.

Conclusion $\pi(x_k) = x_0$

Now let $X_1 = \{x_0, \dots x_k\}$ $Y = \{x \in X \mid x \neq x_0, \dots x_k\}$.

Then π sends x_0 to x_1, x_1 to x_2, $\dots$ x_{k-1} to x_k, x_k to x_0

$\Rightarrow \pi(X_1) = X_1$.

Since π is 1–1, and $\pi(X_1) = X_1$, if $y \notin X_1$ then $\pi(y) \notin X_1$

$\Rightarrow \pi(Y) \subseteq Y$.

Now set

$$\pi_1(x) = \begin{cases} \pi(x) & \text{if } x \in X_1 \\ x & \text{if } x \notin X_1 \end{cases} \qquad \pi_2(x) = \begin{cases} x & \text{if } x \in X_1 \\ \pi(x) & \text{if } x \notin X_1 \end{cases}$$

Then π_1, π_2 are disjoint permutations and

$$\pi = \pi_1 \circ \pi_2$$

Moreover $\pi_2|_Y : Y \to Y$ is a permutation of Y.

(Recall if $f: A \to B$ is a function and $C \subseteq A$, $f|_C : C \to B$ is defined by $(f|_C)(x) = f(x)$ for all $x \in C$)

By inductive assumption $\pi_2|_Y$ is a product of disjoint cycles. We can view each of these cycles as a permutation of X. By construction $\pi_1 : X \to X$ is a cycle.

$\Rightarrow \pi = \pi_1 \circ \pi_2$ is a product of disjoint cycles.

(Uniqueness) Suppose $\pi \in Sym(X)$,

$$\pi = \tau_1 \circ \cdots \circ \tau_r = \sigma_1 \circ \cdots \circ \sigma_\ell$$

τ_i's are disjoint cycles, σ_j's are disjoint cycles.

Then $\tau_1 = (x_0 \ldots x_k)$ for some $x_0 \in X$, $k \in \mathbb{N}$

with $x_1 = \pi(x_0)$, $x_2 = \pi(x_1)$, .. etc.

Since $x_1 \neq \pi(x_0)$, $\exists\ \sigma_j$ s.t $\sigma_j(x_0) \neq x_0$.

No loss of generality to assume: $\sigma_1(x_0) \neq x_0$.

Then $\sigma_j(x_0) = x_0$ for $j > 1$.

$\Rightarrow$ $x_1 = \pi(x_0) = (\sigma_1 \circ \cdots \circ \sigma_\ell)(x_0) = \sigma_1(\sigma_2(\cdots(\sigma_\ell(x_0))\cdots)$

$= \sigma_1(x_0)$ (Since $\sigma_j(x_0) = x_0$ for all $j > 1$)

Since $x_0 \neq x_1$, and σ_1 is 1-1, $x_1 = \sigma_1(x_0) \neq \sigma_1(x_1)$

$\Rightarrow$ τ_1 moves x_1, $\Rightarrow$ $\sigma_2, \ldots \sigma_\ell$ fix x_1.

$\Rightarrow$ $x_2 = \pi(x_1) = (\sigma_1 \circ \cdots \circ \sigma_\ell)(x_1) = \sigma_1(x_1)$

Continue arguing this way (this is really an induction on k, the length of the cycle τ_1)

we see that

$$\tau_1 = (x_0, \ldots x_k)$$

$\Rightarrow$ $\tau_2 \circ \cdots \circ \tau_r$, $\sigma_2 \circ \cdots \circ \sigma_\ell$ map $Y = X \setminus \{x_0 \ldots x_k\}$

$$= \{x \in X \mid x \neq x_0, \ldots x_k\}$$

to itself. and $\tau_2 \circ \cdots \circ \tau_r = \sigma_2 \circ \cdots \circ \sigma_\ell$ in $Sym(Y)$

We want to show: $r = \ell$ and, $\tau_1 = \sigma_1$, $\tau_2 = \sigma_2$, $\ldots$ $\tau_r = \sigma_r$ perhaps after reordering.

We induct on r.

By inductive assumption, $r - 1 = \ell - 1$, and, after reordering σ_j's, $\tau_2 = \sigma_2$, $\tau_3 = \sigma_3$ $\ldots$ $\tau_r = \sigma_r$.

□

Next topic Divisibility of integers (1.6 in Goodman)

Def An integer a *divides* an integer b if $\exists\ q \in \mathbb{Z}$ so that $b = qa$

We write $a \mid b$.
We write $a \nmid b$ if no such q exist.

Ex $3 \mid 6$ $(-3) \mid 6$, $3 \nmid 7$.

Note For any $a \in \mathbb{Z}$, (i) $a \mid a$ since $a = 1 \cdot a$
(ii) $a \mid 0$ since $0 = 0 \cdot a$.

Definition $p \in \mathbb{Z}$ is *prime* if
1) $p \geq 2$ and
2) if $d \mid p$ and $d > 0$, then $d = 1$ or p.

Note By definition 1 is *not* a prime

We will prove:

Prop 1.6.4 Every integer $n \geq 2$ is a prime or a product of primes
Thm 1.6.8 Factorization into primes is unique (up to an order of factors)

We will need:

Well-ordering principle Every nonempty set of non-negative integers has the smallest element.

Remark Well-ordering principle $\Leftrightarrow$ the principle of mathematical induction.
We won't prove this, but it's not hard.