Math 332 Tuesday 2/8/09

Today:
* return HW
* cyclic groups
* permutation groups

* Return HW and discuss.

Cyclic groups C_n a group generated by a single element a of order n.

Last time * $a^k = e$ iff k is a multiple of n.

Cor $a^i = a^j$ iff $i \equiv j \bmod n$.

Prop. Every subgroup of C_n is cyclic.

Pf/ Let $\{1\} \neq H < C_n$, and let k be the smallest positive integer such that $a^k \in H$. Claim: $H = \langle a^k \rangle$. Suppose $a^l \in H$ with $l > k$.

By the division algorithm, we can write $l = qk + r$ with $0 \leq r < k$.

Then $a^l = a^{qk} a^r \in H \Rightarrow a^r = a^l (a^{qk})^{-1} \in H$. But $0 \leq r < k \Rightarrow$ $r = 0$ by definition of k. So $a^l = (a^k)^q \in \langle a^k \rangle$. □

Prop $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$

Pf/ $k = l \gcd(k,n)$ for some $l \in \mathbb{Z} \Rightarrow a^k \in \langle a^{\gcd(k,n)} \rangle$.

Conversely, by the Euclidean algorithm, $\gcd(k,n) = pk + qn$ for some $p, q \in \mathbb{Z}$. Hence, $a^{\gcd(k,n)} = a^{pk} a^{qn} = a^{pk} (a^n)^q = (a^k)^p \in \langle a^k \rangle$. □

Prop $|a^k| = \dfrac{n}{\gcd(k,n)}$

Pf/ Let $d = \gcd(k,n)$. First, note that $a^{k(\frac{n}{d})} = (a^n)^{\frac{k}{d}} = (1)^{k/d} = 1$.

(integer: $\frac{k}{d}$)

Next, $a^{ki} = e \Rightarrow ki = jn$ for some $j \in \mathbb{Z} \Rightarrow i = \frac{jn}{k} = \frac{j(n/d)}{(k/d)}$

(integers: $\frac{k}{d}$, $\frac{n}{d}$)

$\Rightarrow i$ is a multiple of $\frac{n}{d}$. □

Prop The distinct subgroups of C_n are $\{\langle a^k\rangle : 1 \le k \le n,\ k \mid n\}$

↖ k divides n

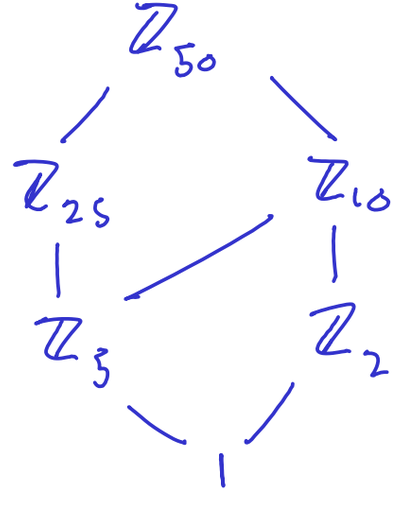
Pf/ We've seen that every subgroup of C_n has the form $\langle a^k\rangle$. Since $\langle a^k\rangle = \langle a^{\gcd(k,n)}\rangle$, we may assume $1 \le k \le n$ and $k \mid n$. Then k is determined exactly by $|a^k|$ since, in this case,

$$|a^k| = \frac{n}{\gcd(k,n)} = \frac{n}{k} \Rightarrow k = |\langle a^k\rangle| / n. \quad \square$$

Examples

* Lattice of subgroups of $\mathbb{Z}_{50}$:

$50 = 2 \cdot 5^2$



* In $\mathbb{Z}_{50}$, $\langle 15\rangle = \langle \gcd(15,50)\rangle$

$= \langle 5\rangle$

$|\langle 15\rangle| = \frac{50}{5} = 10.$

Permutations

(ij), i.e. swapping 2 elements

Parity Every permutation is a product of transpositions.

For example, $(12345) = (15)(14)(13)(12)$. The expression as a product of transpositions is not unique, e.g. $(12345) = (15)(14)(13)(34)(12)(34)$, but the parity (evenness or oddness) of the number of transpositions required is unique. This parity is called the parity of the permutation.

To be proved below

Unfortunate fact An odd (resp. even) length cycle has even (resp. odd) parity. This can be seen in the example above.

Example $\sigma = (132)(4795)(68)$: even · odd · odd = even

odd length ⇒ even parity; odd; odd

Def The sign of a permutation is 1 if it has even parity or -1 if it has odd parity.

Example: For σ as above, $\operatorname{sgn}(\sigma) = 1$.

Proof that parity is well-defined

Let $\sigma \in S_n$. Starting with the identity matrix I_n, permute the rows according to σ to form a matrix P_σ. If e_i is the i^{th} standard basis vector, then $P_\sigma e_i = e_{\sigma(i)}$.

Example $\sigma = (132)$, $P_\sigma = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$,

$P_\sigma e_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = e_3$

$P_\sigma e_2 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = e_1$

$P_\sigma e_3 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = e_2$

$e_1 \mapsto e_3$
$e_2 \mapsto e_1$
$e_3 \mapsto e_2$
(132)

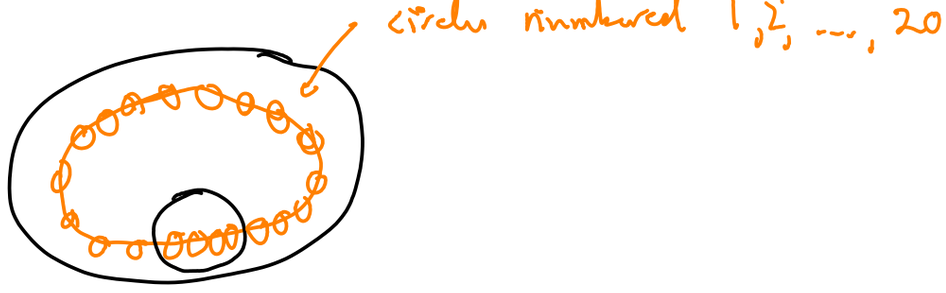
Matrices formed by permuting the rows of I_n are called permutation matrices.

We get a bijection $f: S_n \to \{n \times n \text{ permutation matrices}\}$

Further, $f(\sigma\tau) = f(\sigma)\, f(\tau)$.

Now $\det(I_n) = 1$, and if P is obtained by swapping 2 rows, then $\det(P) = -1$. So $\sigma \in S_n$ is even iff $\det(f) = 1$ and odd iff $\det(P) = -1$. Hence, evenness and oddness of a permutation is well-defined. □

20-game



The puzzle can be thought of as the permutation group generated by $(14)(23)$ and $(1, 2, \ldots, 20)$. Using Sage it's easy to check that this group is, in fact, S_{20}. The group generated by $(14)(23)$ and $(1, 2, \ldots, 19)$ is only $\frac{1}{2}$ of S_{19}, namely the alternating group, A_{19}.

Question: In the 20-game, what is the shortest word in the 2 generators that gives the transposition, $(1,2)$?