

Homework 3

due Monday June 15

Problem 1.

- a) If $U(n)$ is cyclic, how many generators does it have?
- b) Let $k \geq 3$. Prove that $U(2^k)$ is not cyclic.
- c) Determine all nonzero values of $\varphi_{U(n)}$ for $n = 15$ and $n = 21$.

Problem 2. If G is a group, then its *center* $Z(G)$ is set of all elements that commute with everything, while the *derivative* G' is the subgroup generated by all commutators. The center and the derivative can be seen as measuring the “abelianness” of a group.

In this problem, you will compute the center and derivative of the finite dihedral group D_n .

- a) Show that $[r^i, r^j] = e$.
- b) Show that $[fr^i, fr^j] = r^{2(j-i)}$.
- c) Show that $[r^i, fr^j] = r^{2i}$.
- d) Conclude that $D_n' = \langle r^2 \rangle$. What is $[D_n : D_n']$ for all $n \geq 1$?
- e) Use the above calculations to determine $Z(D_n)$ (with justification) for all $n \geq 1$.

Problem 3. Let G be a group.

- a) Let [IOTA] $\iota(x) = x^{-1}$ for all x in G .
 - i. Show that $\iota \in \text{Sym}(G)$.
 - ii. Suppose G has order n and let $a = \varphi_G(2)$. What is the cycle type of ι ?
 - iii. Deduce that if G has even order then G has an element of order 2.
- b) Fix $g \in G$ and define [RHO] $\rho(x) = gx$ for all x in G .
 - i. Show that $\rho \in \text{Sym}(G)$.
 - ii. Suppose G has order n and let $b = o(g)$. What is the cycle type of ρ ?
 - iii. Deduce that $o(g) \mid o(G)$ *without* appealing to Lagrange’s Theorem.

Problem 4. Fill in the following table for S_6 like we did for S_5 in Lecture 11.

partition	cycle type	order	number
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Using the table, determine $\varphi_{S_6}(d)$ for all d . What is $\exp(S_6)$?

Problem 5. Find explicit elements of $S_\infty = \text{Sym}(\mathbb{N})$ with the following cycle types:

- a) $(1, 1, 1, \dots; 0)$ b) $(0, 0, 0, \dots; 1)$ c) $(1, 1, 1, \dots; 1)$ d) **(bonus)** $(0, 0, 0, \dots, \infty)$.

[Your answers must be unambiguous. That does not mean you need to come up with formulas or piecewise definitions; you just need to make it clear what the output would be given any positive integer input. For example, you can write out a small part of each permutation (using two-line or cycle notation) and indicate the pattern or the rest of the definition in words. No proofs required. The bonus must be flawless to count as correct.]

Extra Problems

not to be submitted

Extra Problem 1. Do all the Exercises from Lectures 8–12.

Extra Problem 2 (Guises of D_n).

- a) Let G be the group of invertible maps of the form

$$x \mapsto ax + b$$

with $a, b \in \mathbb{Z}$. Prove that G is dihedral.

- b) Let G be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/n)$ generated by the matrices

$$\begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \overline{-1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}.$$

Prove that G is dihedral of order $2n$ for $n \geq 3$.

- c) Let $a \in \mathbb{C}^\times$. Show that the maps $z \mapsto az$ and $z \mapsto \bar{z}$ generate a dihedral subgroup of $\mathrm{Sym}(\mathbb{C})$. When is it finite?

Extra Problem 3 (Tower Law for Indices). Let $K \leq H \leq G$ be finite groups. Prove that

$$[G : K] = [G : H][H : K].$$

Can you do it for infinite groups?

Extra Problem 4. In this problem, you will give a rigorous proof of the fact that $o(S_n) = n!$ using only group theory.

- a) We can regard each S_n as a subset of S_∞ by setting $\sigma(k) = k$ for all $k > n$ (“extension by the identity”). Show that, from this point of view, $S_n \leq S_{n+1}$ for all $n \geq 1$.
- b) Let $\sigma, \tau \in S_n$. Show that $\sigma S_{n-1} = \tau S_{n-1}$ iff $\sigma(n) = \tau(n)$.
- c) Prove that $[S_n : S_{n-1}] = n$ for all $n > 1$.
- d) Use the tower law for indices to compute $[S_n : S_1]$.
- e) Deduce that $o(S_n) = n!$.

Extra Problem 5. Let G be a group.

- a) Assume G has order n . For each integer k define $\pi_k(x) = x^k$ for all x in G .
- i. Suppose $\gcd(k, n) = 1$. Show that $\pi_k \in \mathrm{Sym}(G)$.
- ii. Define the G -symbol as the function $\mathbb{Z} \rightarrow \{-1, 0, 1\}$ given by

$$\left(\frac{k}{G}\right) = \begin{cases} \mathrm{sgn}(\pi_k) & \text{if } \gcd(k, n) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Prove that $\left(\frac{1}{G}\right) = 1$.

iii. Prove that

$$\left(\frac{k}{G}\right) = \left(\frac{k'}{G}\right)$$

if $k \equiv k' \pmod{n}$ [i.e. the G -symbol is n -periodic].

iv. Prove that

$$\left(\frac{kk'}{G}\right) = \left(\frac{k}{G}\right) \left(\frac{k'}{G}\right)$$

if $\gcd(k, k') = 1$ [i.e. the G -symbol is multiplicative].

v. Show that if k is a nonzero square modulo p , then

$$\left(\frac{k}{\mathbb{Z}/p}\right) = 1.$$

vi. Evaluate

$$\left(\frac{k}{D_4}\right)$$

for each k in $\mathbb{Z}$.

b) Fix $g \in G$ and define [KAPPA] $\kappa(x) = gxg^{-1}$ for all x in G .

i. Show that $\kappa \in \text{Sym}(G)$.

ii. Show that $\text{Fix}(\kappa) \leq G$.

iii. Suppose G has order n . Show that $c_1 \mid n$.

iv. What is the cycle type of κ ?

Extra Problem 6. Suppose σ has cycle type $(c_1, \dots; c_\infty)$. What is the cycle type of σ^2 ? Adhere to the usual conventions regarding ∞ , namely $\infty + n = n + \infty = \infty$ for all n and $m \cdot \infty = \infty \cdot m = \infty$ for all $m > 0$.