Problem Set 1

Exercises with (HW) are due Friday 9/6 in class. Your homework should be easily legible, but need not be typed in Latex. Use full sentences to explain your solutions, but try to be concise as well.

Exercises for Wednesday, 8/28

Exercises 1.1. An alternative version of the QR Theorem.

(a) Let a and b be integers with $b \neq 0$. There exist unique integers q, r such that

(1) $a = bq + r$, and

(2) $|b|/2 < r \leq |b|/2$

[There are two approaches: use the existing QR Theorem to prove the alternative, or prove it from scratch by redefining S and modifying the proof of the QR Theorem.]

Exercises 1.2. The Euclidean algorithm

(a) Use the matrix version of the Euclidean algorithm to express the greatest common divisor of 89 and 24 as a linear combination of 89 and 24.

Exercises 1.3. A consequence of unique factorization

(a) Every nonzero rational number a can be uniquely expressed in the form

$$a = up_1^{e_1} \cdots p_t^{e_t}$$

for some $u = \pm 1$, $t \in \mathbb{N}_0$, prime numbers $p_1 < p_2 < \cdots < p_t$, and nonzero integers $e_1, \ldots, e_t$.

Exercises 1.4. Invertible elements in $\mathbb{Z}/n$

(a) Let p be a prime number. Let $[a] \in \mathbb{Z}/p$ with $[a] \neq [0]$ (so a is not divisible by p). Use the GCD Theorem to show there is some $r \in \mathbb{Z}/p$ such that $[a][r] = [1]$ .Consequently, each nonzero element of $\mathbb{Z}/p$ has a multiplicative inverse.

(b) Extend this result, partially, to $\mathbb{Z}/n$ for composite n. If $[a] \in \mathbb{Z}/n$ is such that the integer a is coprime to n, then there is some $[r] \in \mathbb{Z}/n$ such that $[a][r] = [1]$.

Exercises for 9/4

Exercises 1.5. Basic Group Properties.

Let $G, *$ be a group. Give succinct but complete proofs of the following.

(a) The identity element is unique.

(b) The inverse of any element is unique.

(c) The cancellation law holds: $a*b = a*c$ implies $b = c$ (and similarly for cancellation on the right).

(d) If $a * g = g$ for some $g \in G$, then $a = e_G$.

(e) $(a * b)^{-1} = b^{-1} * a^{-1}$.

(f) $(a^{-1})^{-1} = a$.

(g) (HW) If every non-identity element has order 2, then G is abelian.

Exercises 1.6. A Perverse Group

(a) Show that $\mathbb{Z}$ is a group under the operation $\square$ defined by $a \square b = a + b - 2$. (What is the identity element? What is the inverse of an element a?)

(b) (HW) Find an isomorphism from $\mathbb{Z}, +$ to $\mathbb{Z}, \square$.

Exercises 1.7. Formulas for the operations in D_5

The goal of this problem is to find formulas for the product of two arbitrary elements of D_5. We will use arithmetic in $\mathbb{Z}/5$ with the system of representatives $0, 1, 2, 3, 4$.

(a) Observe that the reflection t_i applied to the original position of the pentagon (in Figure 1) switches $i + 1$ with $i - 1$ and $i + 2$ with $i - 2$ where computations are modulo 5. Show that when t_i is applied to the original position of the pentagon the vertex at base point a is $2i - a$. We can write this as $t_i(a) = 2i - a$.

(b) Explain why the product of two reflections is a rotation, and find a formula for $t_i * t_j(a)$.

(c) (HW) Show that $r * t_i = t_{i+3}$ by arguing that $r * t_i$ is a reflection and that, applied to the pentagon in the original position, it takes $i + 3$ to itself.

(d) (HW) Find a formula for $r^j * t_i$; that is, give a function of $\mathbb{Z}/5$ [Hint: linear] for $r^j * t_i(a)$. Do the same for $t_i * r^j$.

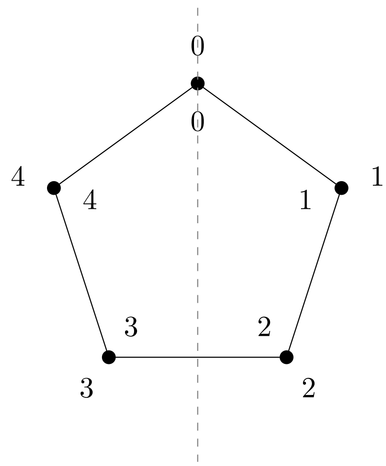


Figure 1: The Pentagon

Exercises 1.8. (HW) Some subgroups of abelian groups

Let A be an abelian group and let m be an integer.

(a) Let $mA = \{ma : a \in A\}$. Show that mA is a subgroup of A.

(b) Let $A[m] = \{a \in A : ma = 0\}$. Show that $A[m]$ is a subgroup of A.

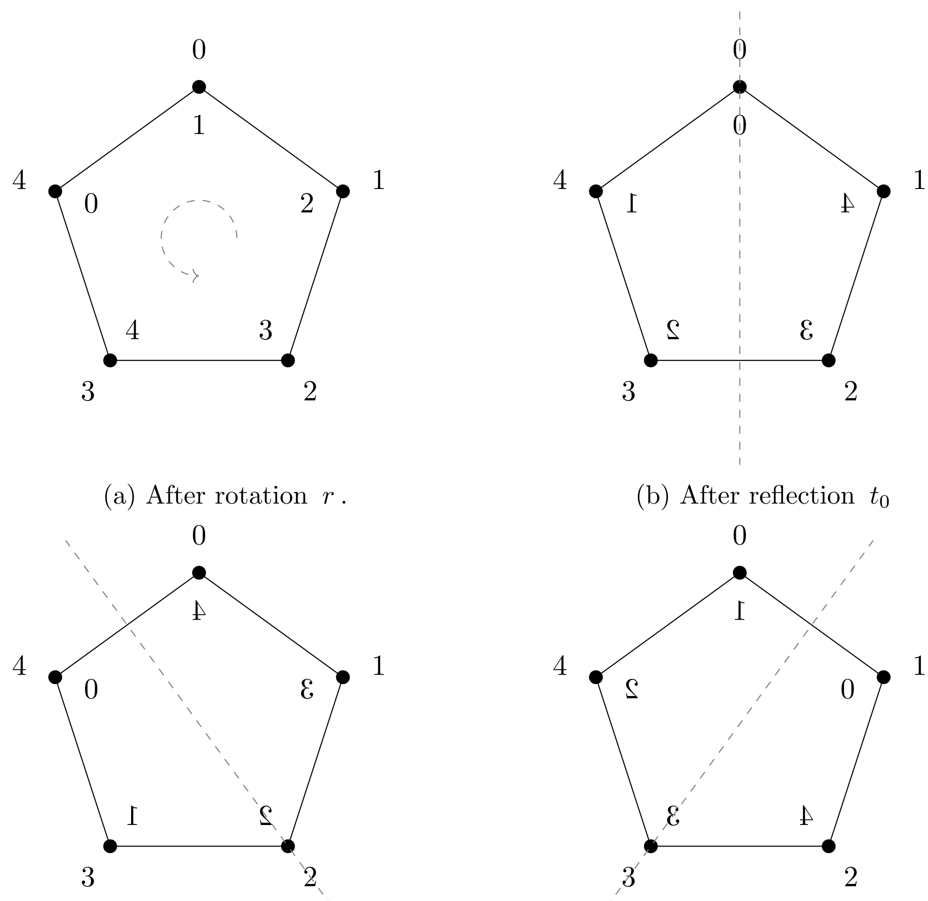
(c) Give an example in which $mA \cap A[m]$ is trivial (just 0) and given an example in which it is not trivial.

Exercises 1.9. (HW) Order and commutativity.

(a) If $g \in G$ has order m and $h \in H$ has order n, find the order of $(g, h) \in G \times H$.

(b) Suppose that $a, b \in G$ commute (that is $ab = ba$). If $\text{ord}(a)$ and $\text{ord}(b)$ are coprime find the order of ab.

(c) Let A be an abelian group with finite exponent. Show that there is some $a \in A$ such that $\text{ord}(a) = \exp(A)$.



(a) After rotation r.

(b) After reflection t_0

(c) After $t_0 r = t_2$.

(d) After $r t_0 = t_3$

Figure 2: The pentagon after various transformations