Problem Set 1

Problems with (HW) are due Friday 9/1 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.

Problems for Wednesday, 8/23 and Friday, 8/25

Problems 1.1. Basic Group Properties. Let $G, *$ be a group. Give succinct but complete proofs of the following.

(1) The identity element is unique.
(2) The inverse of any element is unique.
(3) The cancellation law holds: $a{*}b = a{*}c$ implies $b = c$ (and similarly for cancellation on the right).
(4) If $a * g = g$ for some $g \in G$, then $a = e_G$.
(5) $(a * b)^{-1} = b^{-1} * a^{-1}$.
(6) $(a^{-1})^{-1} = a$.
(7) If every element is of order 2, then G is abelian.

Problems 1.2. A Perverse Group

(1) 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?)
(2) (HW) Find an isomorphism from $\mathbb{Z}, +$ to $\mathbb{Z}, \square$.

Problems 1.3. Use the Euclidean algorithm to express the greatest common divisor as a linear combination of the given integers.

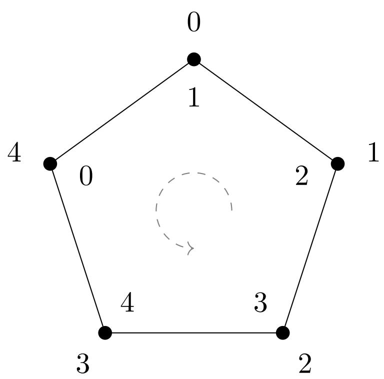
(1) 89, 24

Problems 1.4.

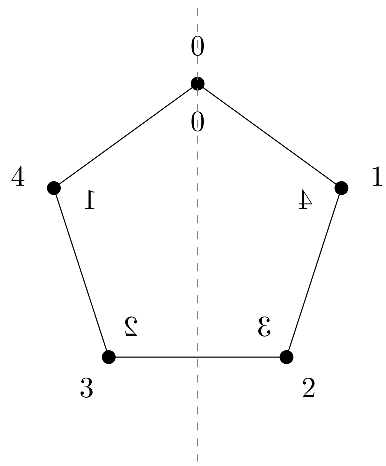
(1) Let p be a prime number. Let $[a] \in \mathbb{Z}/p$ with $[a] \neq [0]$ (so a is not divisible by p). Use the GCD Theorem to show there is some $r \in \mathbb{Z}/p$ such that $[a][r] = [1]$ .Consequently, each nonzero element of $\mathbb{Z}/p$ has a multiplicative inverse.
(2) Extend this result, 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 $[a][r] = [1]$.
(3) What do these results say about generators for the group $\mathbb{Z}_n$ (the integers modulo n, forgetting multiplication).
(4) Show that the elements that have multiplicative inverses in $\mathbb{Z}/n$ form a group under multiplication. It is often denoted U_n.

Problems 1.5. The Dihedral Group D_5. See Section 1.2.

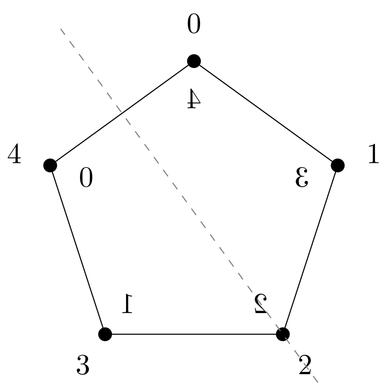
(1) Do 1.2.5 (a), (b) to find a formulas for t_i and simplify rt_i.
(2) (HW) Do 1.2.5 (c), (d). Find a formula for $r^j t_i$ and for $t_i t_j$.



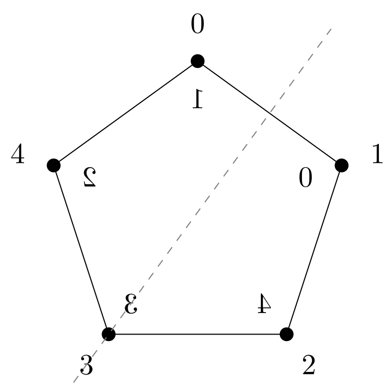
(a) After rotation r.



(b) After reflection t_0



(c) After $t_0 r = t_2$.



(d) After $rt_0 = t_3$

Figure 1: The pentagon after various transformations

Problems 1.6. (HW) Some subgroups of abelian groups. Let A be an abelian group and let m be an integer.

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

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

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

Exercises 1.7. (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 $\text{ord}(a) = \exp(A)$.