Nathan Bickel
MATH 701: Section 001
Professor: Dr. Tsai
September 8, 2024

MATH 701 Homework 1

Problem 1.1.9 Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.

(a) Prove that G is a group under addition.

(b) Prove that nonzero elements of G are a group under multiplication.

(a) We prove each axiom:

- **Closure:** Let $x = a + b\sqrt{2}$, $x' = a' + b'\sqrt{2} \in G$. Then

$$x + x' = (a + a') + (b + b')\sqrt{2},$$

  so $x + x' \in G$ by closure of addition in $\mathbb{Q}$.
- **Associativity:** Addition is known to be associative.
- **Identity:** If G has an identity, it must be 0, and we have $0 = 0 + 0\sqrt{2} \in G$.
- **Inverses:** Let $x = a + b\sqrt{2}$. Then we define $x^{-1} := -a - b\sqrt{2}$, which is in G by closure of negation in the rationals and satisfies $x + x^{-1} = x^{-1} + x = 0$. So x^{-1} is an inverse.

Therefore, G is a group under addition. □

(b) Let $G^* := G \setminus \{0\}$. We prove each axiom:

- **Closure:** Let $x = a + b\sqrt{2}$, $x' = a' + b'\sqrt{2} \in G^*$. Then

$$xx' = (a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2} \in G.$$

  Since neither x and x' are both nonzero, so is xx', so $xx' \in G$.
- **Associativity:** Multiplication is known to be associative.
- **Identity:** If G^* has an identity, it must be 1, and we have $1 = 1 + 0\sqrt{2} \in G^*$.
- **Inverses:** Let $x = a + b\sqrt{2}$. We define $x^{-1} := \frac{a - b\sqrt{2}}{a^2 + 2b^2}$, which is clearly in G^* and satisfies

$$xx^{-1} = \left(a + b\sqrt{2}\right)\left(\frac{a - b\sqrt{2}}{a^2 + 2b^2}\right) = \frac{a^2 + 2b^2}{a^2 + 2b^2} = 1.$$

  Since $x^{-1}x = xx^{-1} = 1$ follows from commutativity of multiplication, x^{-1} is an inverse. □

Therefore, the nonzero elements of G are a group under multiplication. □

Problem 1.1.22 If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Let $x, g \in G$. Let $k := |x|$ and $k' := |g^{-1}xg|$. We have $x^k = 1$, so applying associativity/inverse cancellation we obtain

$$(g^{-1}xg)^k = g^{-1}x^k g = g^{-1}g = 1$$

and thus $|g^{-1}xg| \leq |x|$. We also have

$$\begin{aligned}
(g^{-1}xg)^{k'} &= 1 && \text{(by choice of } k') \\
\implies g^{-1}x^{k'}g &= 1 && \text{(associativity/inverse cancellation)} \\
\implies g^{-1}x^{k'} &= g^{-1} && \text{(right multiplying by } g^{-1}) \\
\implies x^{k'} &= gg^{-1} && \text{(left multiplying by } g) \\
&= 1, && \text{(inverse cancellation)}
\end{aligned}$$

and thus $|x| \leq |g^{-1}xg|$. Therefore, $|x| = |g^{-1}xg|$.

Let $a, b \in G$, and consider $x := ab$, $g = a$. Then from the result, we have

$$|ab| = |x| = |g^{-1}xg| = |a^{-1}aba| = |ba|.$$

□

Problem 1.1.25 Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

Let $a, b \in G$. Then, we have

$$\begin{aligned}
abab &= 1 && ((ab)^2 = 1 \text{ from assumption}) \\
\implies aabab &= a && \text{(left multiplying by } a) \\
\implies aababb &= ab && \text{(right multiplying by } b) \\
\implies ba &= ab. && (aa = bb = 1 \text{ from assumption})
\end{aligned}$$

Therefore, G is commutative. □

Problem 1.1.28 Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product. Verify all the group axioms for $A \times B$:

(a) Prove that the associative law holds: for all $(a_i, b_i) \in A \times B$, $i \in \{1, 2, 3\}$,

$$(a_1, b_1)\left[(a_2, b_2)(a_3, b_3)\right] = \left[(a_1, b_1)(a_2, b_2)\right](a_3, b_3).$$

(b) Prove that $(1, 1)$ is the identity of $A \times B$.

(c) Prove that the inverse of (a, b) is (a^{-1}, b^{-1}).

(a) We have

$$\begin{aligned}
(a_1, b_1)\left[(a_2, b_2)(a_3, b_3)\right] &= (a_1, b_1)(a_2a_3, b_2b_3) \\
&= \big(a_1(a_2a_3), b_1(b_2b_3)\big)
\end{aligned}$$

$$\begin{aligned} &= \big((a_1a_2)a_3, (b_1b_2)b_3\big) && \text{(by associativity of } \star \text{ and } \diamond\text{)} \\ &= \big[(a_1a_2, b_1b_2)\big]\,(a_3, b_3) \\ &= \big[(a_1, b_1)(a_2, b_2)\big]\,(a_3, b_3). \end{aligned}$$

(b) Let $(a, b) \in A \times B$. We have $(1, 1) \in A \times B$ since $1 \in A$ and $1 \in B$, and we have

$$(a, b)(1, 1) = (a \star 1, b \diamond 1) = (a, b)$$

and

$$(1, 1)(a, b) = (1 \star a, 1 \star b) = (a, b).$$

Therefore, $(1, 1)$ is the identity of $A \times B$.

(c) Let $(a, b) \in A \times B$. Since A and B are groups, there must exist inverses $a^{-1} \in A$ and $b^{-1} \in B$, so $(a^{-1}, b^{-1}) \in A \times B$. We have

$$(a, b)(a^{-1}, b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (1, 1)$$

and

$$(a^{-1}, b^{-1})(a, b) = (a^{-1} \star a, b^{-1} \diamond b) = (1, 1),$$

so the inverse of (a, b) is (a^{-1}, b^{-1}). □

Problem 1.2.3 We have that D_{2n} has the usual presentation $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1}\rangle$. Use these generators and relations to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.

We first prove a lemma: every $\sigma \in D_{2n}$ can be expressed as either r^k or sr^k for some $k \in [n]$.

Proof. Let $\sigma = a_1^{k_1}a_2^{k_2}\dots a_m^{k_m} \in D_{2n}$, where for all $i \in [m]$, $a_i \in \{r, s\}$ and $k_i \in \mathbb{Z}$. We can assume that the a_i's alternate between r and s (if not, we can rewrite it in this way by combining the powers). We can replace each $a_i = s^{k_i}$ with either e or s, since s has order 2. Since we are given that $rs = sr^{-1}$, we can "shift" all the instances of s to the left until they all collect at the left without changing anything other than the powers of the instances of r (this can be shown easily with induction). The product of the s's can be written as either e or s since $s^2 = 1$, and the product of the r's can be r^k for some $k \in [n]$ since $r^n = 1$. Therefore, we either have $\sigma = r^k$ or $\sigma = sr^k$.

We now prove that every element of D_{2n} which is not a power of r has order 2. By the lemma, the only such element is sr^k for some $k \in [n]$. We have $r^k s = sr^{-k}$ by repeated application of $rs = sr^{-1}$, so we have

$$(sr^k)(sr^k) = s(r^k s)r^k = s(sr^{-k})r^k = (ss)(r^{k-k}) = e,$$

so $|r^k s| \leq 2$. Since $r^k s$ is not the identity, we have $|r^k s| \geq 2$ and thus the order of the element is 2.

Clearly, D_{2n} is generated by s and sr since $r = s(sr)$. Both of these elements have order 2 as they are not powers of r.

Problem 1.2.9 Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.

Let v_1, v_2, v_3, v_4 be the vertices of the tetrahedron. A motion can map v_1 to any of the four vertices, and for each of these motions, there are three choices for the other three vertices by rotating them about the line going through v_1. Therefore, there are $3 \cdot 4 = 12$ motions and $|G| = 12$. □

Problem 1.2.10 Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.

Let $f_1, f_2, f_3, f_4, f_5, f_6$ be the faces of the cube. A motion can map f_1 to any of the six faces, and for each of these mappings, the cube can be rotated four times about the line going through f_1. Therefore, there are $6 \cdot 4 = 24$ motions and $|G| = 24$. □

Problem 1.3.2 Let σ be the permutation

$1 \mapsto 13$	$2 \mapsto 2$	$3 \mapsto 15$	$4 \mapsto 14$	$5 \mapsto 10$
$6 \mapsto 6$	$7 \mapsto 12$	$8 \mapsto 3$	$9 \mapsto 4$	$10 \mapsto 1$
$11 \mapsto 7$	$12 \mapsto 9$	$13 \mapsto 5$	$14 \mapsto 11$	$15 \mapsto 8$

and let τ be the permutation

$1 \mapsto 14$	$2 \mapsto 9$	$3 \mapsto 10$	$4 \mapsto 2$	$5 \mapsto 12$
$6 \mapsto 6$	$7 \mapsto 5$	$8 \mapsto 11$	$9 \mapsto 15$	$10 \mapsto 3$
$11 \mapsto 8$	$12 \mapsto 7$	$13 \mapsto 4$	$14 \mapsto 1$	$15 \mapsto 13.$

Find the cycle decompositions of the following permutations: σ, τ, σ^2, $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

We have:

- $\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)$
- $\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)$
- $\sigma^2 = (1\ 5)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14)(10\ 13)$
- $\sigma\tau = (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14)$
- $\tau\sigma = (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14)$
- $\tau^2\sigma = (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)$

Problem 1.3.6 Write out the cycle decomposition of each element of order 4 in S_4.

The only elements of order 4 in S_4 are the 4-cycles (the composition of two 2-cycles will have order 2). They are:

- $(1\ 2\ 3\ 4)$
- $(1\ 2\ 4\ 3)$
- $(1\ 3\ 2\ 4)$
- $(1\ 3\ 4\ 2)$
- $(1\ 4\ 2\ 3)$
- $(1\ 4\ 3\ 2)$

Problem 1.3.10 Prove that if σ is the m-cycle $(a_1\, a_2\, \ldots\, a_m)$, then for all $i \in \{1, 2, \ldots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k + i$ is replaced by its least residue mod m when $k + i > m$. Deduce that $|\sigma| = m$.

We have $\sigma(a_k) = a_{k+1}$ (with replacing $k+1$ by least residue mod m when $k+1 > m$) by definition, and a straightfoward induction proof shows that the same holds for $i > 1$. Since $m + k \equiv k \pmod{k}$, we have $\sigma^m(a_k) = a_k$ and thus $|\sigma| \leq m$. Since $m + k$ is the least natural number greater than k equivalent to $k \pmod{m}$, we have $|\sigma| = m$. □

Problem 1.3.15 Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.

Let $\sigma \in S_n$, and let m be the least common multiple of the lengths of the cycles in the cycle decomposition of x. Since m is a multiple of the length of every cycle, we can combine Problem 1.3.10 with the commutativity of disjoint cycles to see that each cycle will be the identity. Thus, $|\sigma| \leq m$. For any $m' < m$, m' will not be a multiple of at least one of the lengths of the cycles, so this cycle raised to m' will not be the identity. Since the cycles are disjoint, the cycle decomposition raised to m' will also not be the identity, so $|\sigma| \geq m$. Therefore, $|\sigma| = m$. □