Dartmouth College Department of Mathematics
Math 71 Algebra
Fall 2025

Problem Set # 1 (due via Canvas upload by 5 pm, Wednesday, October 1)

Notation: Given positive integers $a_1, \ldots, a_n$ we define their **least common multiple** $\mathrm{lcm}(a_1, \ldots, a_n)$ to be least positive integer that is divisible by each of $a_1, \ldots, a_n$. The following characterization of the lcm is useful:

If $N \geq 1$ is a multiple of a_i for all $i = 1, \ldots, n$ then $\mathrm{lcm}(a_1, \ldots, a_n)$ divides N.

By the way, to show that two positive integers n and m are equal, it suffices to show that n divides m and that m divides n.

Reading: DF 0.2–0.3, 1.1–1.5.

Problems: (Only DF *ed problems non-DF problems will be graded, but you should solve them all.)

1. Read DF 0.2 (5)–(7) about the Euclidean Algorithm and the last paragraph in DF 0.3 about how to compute inverses modulo n using the Euclidean Algorithm. Then complete the following practice exercises: DF 0.2 Exercises 1ab, DF 0.3 Exercises 15ab.

2. Let G be a group and $a_1, a_2, \ldots, a_r \in G$. We say that $a_1, \ldots, a_r$ **pairwise commute** if a_i commutes with a_j for all i and j. We say that $a_1, \ldots, a_r$ are **rank independent** if $a_1^{e_1} \cdots a_r^{e_r} = 1$ implies that e_i is a multiple of $|a_i|$ for all i. The aim of the problem is to prove:

Proposition. *Let G be a group and $a_1, a_2, \ldots, a_r \in G$ be pairwise commuting rank independent elements of finite order. Then $|a_1 \cdots a_r| = \mathrm{lcm}(|a_1|, \ldots, |a_r|)$.*

(a) (DF 1.1 Exercise 24) If a and b are commuting elements, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. Hint: Do induction on n.

(b) If $a_1, \ldots, a_r$ are pairwise commuting elements, prove that $(a_1 \cdots a_r)^n = a_1^n \cdots a_r^n$. Hint: Do induction on r.

(c) If $a_1, \ldots, a_r$ are pairwise commuting elements of finite order (not necessarily rank independent), prove that $|a_1 \cdots a_r|$ divides $\mathrm{lcm}(|a_1|, \ldots, |a_r|)$. Hint: Raise $a_1 \cdots a_r$ to the power $\mathrm{lcm}(|a_1|, \ldots, |a_r|)$.

(d) Prove the proposition. Hint: Do induction on r; for the base case $r = 1$ there is not much to say, and then you should realize that (after a bit of juggling with least common multipliers) the induction step just boils down to the case $r = 2$. Hint (for a different proof): Use the above characterization of the lcm to prove that $\mathrm{lcm}(|a_1|, \ldots, |a_n|)$ divides $|a_1 \cdots a_n|$. In any method you choose, be sure to highlight where the rank independence condition is used!

(e) Show that disjoint cycles in S_n are rank independent, then deduce DF 1.3 Exercise 15.

3. DF 1.2 Exercises 2, 3*, 7*. Look at 9–13.

DF 1.3 Exercises 1 (also compute the order of each permutation), 10* ("least positive residue mod m" means a number between 1 and m, not between 0 and $m-1$ as we are used to taking residues), 11*, 13*, 16.

DF 1.4 Exercises 4*, 8, 11abde*.

DF 1.5 Exercises 1, 2.

DF 1.6 Exercises 1, 2*, 3, 4*, 6*, 7, 9* (here D_{24} is the dihedral group with 24 elements).

4. Let $d \in \mathbb{Z}$ be a nonsquare. Prove that $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$ is a field under addition and multiplication of complex numbers. **Hint.** You can take it for granted that $\sqrt{d}$ is irrational.

5. Remind yourself (or learn about) the field of complex numbers $\mathbb{C} = \{z = x + iy \ : \ x, y \in \mathbb{R},\ i^2 = -1\}$. Prove that complex conjugation $z = x + iy \mapsto \overline{z} = x - iy$ is a homomorphism of the additive group $\mathbb{C} \to \mathbb{C}$ and the multiplicative group $\mathbb{C}^\times \to \mathbb{C}^\times$. Prove that the absolute value $z \mapsto |z| = \sqrt{z\,\overline{z}}$ is a homomorphism of multiplicative groups $\mathbb{C}^\times \to \mathbb{R}^\times$. Let $U = \{z \in \mathbb{C} \ : \ |z| = 1\}$ be the unit circle. Prove that the map $\mathbb{R} \to U$ defined by $\theta \mapsto e^{i\theta}$ is a group homomorphism.