Problem Set # 1 (due at the beginning of class on Friday 16 September)

Notation: Given positive integers \(a_1, \ldots, a_n\) we define their least common multiple \(\text{lcm}(a_1, \ldots, a_n)\) 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 \(\text{lcm}(a_1, \ldots, a_n)\) 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 1.1–1.6.

Problems: (Starred* problems in DF are strongly recommended!)

1. 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 \(|a_1 \cdots a_r| = \text{lcm}(|a_1|, \ldots, |a_r|)|.\)

(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 \(\text{lcm}(|a_1|, \ldots, |a_r|)\). Hint: Raise \(a_1 \cdots a_r\) to the power \(\text{lcm}(|a_1|, \ldots, |a_r|)\).

(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 \(\text{lcm}(|a_1|, \ldots, |a_n|)\) 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.

2. DF 1.2 Exercises 2, 3*, 7*.

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*.

DF 1.4 Exercises 2, 4*, 5.

3. DF 1.6 Exercises 2*, 3, 4*, 6*, 7, 9* (here \(D_{24}\) is the dihedral group with 24 elements), 14*, 16, 17* (prove that it’s always a bijection), 18, 24*, 25.