Yale University Department of Mathematics

Math 350 Introduction to Abstract Algebra

Fall 2015

Problem Set # 1 (due at the beginning of class on Friday 18 September)

Notation: If S is a set of elements (numbers, rabbits, ...) then the notation "$s \in S$" means "s is an element of the set S." If T is another set, then the notation "$T \subseteq S$" means "every element of T is an element of S" or "T is a **subset** of S." We can specify a subset $T \subset S$ by conditions on the elements of S, e.g., if S is the set of rectangles, then the subset of squares is $\{s \in S \mid \text{all sides of } s \text{ have the same length}\}$. If S and T are sets, then a **function** or **map** $f : S \to T$ from S to T is the a rule that associates to each element $s \in S$, an element $f(s) \in T$.

Reading: DF 0.1–0.3, 1.1–1.6.

Problems:

1. DF 0.1 Exercises 5, 7.
DF 0.2 Exercises 3, 7, 10, 11.
DF 0.3 Exercises 4, 7, 8, 10, 13.

2. DF 1.1 Exercises 9, 14, 20, 22, 25, 31.

3. 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, 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 $r = 2$.
(e) Show that disjoint cycles in S_n are rank independent, then deduce DF 1.3 Exercise 15.

4. DF 1.2 Exercises 2, 3, 7.
DF 1.3 Exercises 1 (also compute the order of each permutation), 5, 10, 11, 13.
DF 1.4 Exercises 2, 4, 5.

5. DF 1.6 Exercises 2, 3, 4, 6, 7, 9, 14, 16, 17 (prove that it's always a bijection), 18, 23, 24, 25.
DF 1.7 Exercises 5, 17 (this gives another proof of 1.1 Exercise 22), 18, 19.

6. Prove that if G is a group and $a, b \in G$ satisfy $ab = e$ then a is the inverse of b and b is the inverse of a, i.e., a left (or right) inverse is actually an inverse in a group. Prove that if $ga = a$ for all $a \in G$ or that $ag = a$ for all $a \in G$, then g is the identity, i.e., a left (or right) identity is actually an identity in a group.

Yale University, Department of Mathematics, 10 Hillhouse Ave, New Haven, CT 06511
E-mail address: asher.auel@yale.edu