Math 103A, Fall 2019

Modern Algebra I, HW 2

Due Friday October 18th at 11:30AM in Ji Zeng's box outside B402A.

From Armstrong's Groups and Symmetry:

- Exercises (Chapter 2, pages 9–10):

  2.7

- Exercises (Chapter 3, pages 13–14):

  3.3, 3.4, 3.7

Problem A. Let $(G, *)$ be a group. Associated with each element $a \in G$ there is a function from G to itself which we denote $r_a : G \longrightarrow G$ given by the recipe

$$r_a(x) == x * a \qquad \forall x \in G.$$

(Think of r_a as multiplication-by-a on the right.)

(a) Verify in detail that r_a is bijective for all $a \in G$.

(b) For any two elements $a, b \in G$ show that the following relation holds:

$$r_{a*b} == r_b \circ r_a.$$

(On the right-hand side $\circ$ denotes composition of functions.)

Problem B.

(a) Let $(G, *)$ be a group with three elements $\{e, a, b\}$ (of which e is the neutral element). Explain why we must have $a * b = e$, and use this observation to fill out the entire composition table.

(b) Now let $(G, *)$ be a group with four elements $\{e, a, b, c\}$. Show that either $a * b = e$ or $a * b = c$. Assuming $a * b = e$ complete the composition table.

(c) In continuation of part (b) – in the case where $a * b = c$ complete the composition table under the additional assumption that $a^2 = b^2 = c^2 = e$.

Problem C. Let $\mathbb{Z}_{43}^{\times}$ denote the (multiplicative) group of all invertible residue classes modulo 43.

(a) Find its cardinality $|\mathbb{Z}_{43}^{\times}|$.

(b) Compute the following products in $\mathbb{Z}_{43}^{\times}$:

$$[2] \bullet [5], \qquad [3] \bullet [17], \qquad [11] \bullet [13], \qquad [-7] \bullet [19].$$

(Express your answers in the form $[x]$ with $x \in \mathbb{Z}$ in the range $0 \leq x < 43$.)

(c) Explain why $[41]$ belongs to $\mathbb{Z}_{43}^{\times}$ and find its inverse class: Find the $x \in \mathbb{Z}$ in the range $0 \leq x < 43$ satisfying the congruence $41x \equiv 1 \pmod{43}$.

Problem D.

(a) Calculate $\phi(385)$. (Here ϕ denotes Euler's function.)

(b) Find the general solution to the following system of congruences:

$$x \equiv 1 \pmod{5} \quad \wedge \quad x \equiv 2 \pmod{7} \quad \wedge \quad x \equiv 3 \pmod{11}.$$

(c) For the system in (b) list all solutions $x \in \mathbb{Z}$ with $|x| < 400$.