MA 541: Modern Algebra I / Fall 2021
Homework assignment #4
~~Due WEDNESDAY 10/13/21 before 5pm~~
Due THURSDAY 10/14/21 before 12pm

Three ways to turn in your work on the due date: in class, before ~~5pm~~ 12pm in the envelope hanging on MCS 127, or before ~~5pm~~ 12pm emailed as an attachment to `buma541f2021@gmail.com`.

- If you handwrite your solutions, please try to turn in the original rather than email a scan; also, please staple or otherwise connect the pages of your work. Definitely write your name on the front page.
- If you email, please have the filename identify you, the homework number, and this course, in that order.
- **Challenge problems:** Please turn solutions to challenge problems in separately. You may also turn in challenge problems later, after the deadline on the main set.

(1) Consider the set $\mathrm{GL}_2(\mathbb{Z}_2)$ of invertible 2×2 matrices with coefficients in $\mathbb{Z}_2$. Convince yourself that this is a group under multiplication.

(a) List the elements of $\mathrm{GL}_2(\mathbb{Z}_2)$. How many are there?

(b) Give the group table for $\mathrm{GL}_2(\mathbb{Z}_2)$.

(c) Is there another group G that we have studied with the same Cayley table up to relabeling as $\mathrm{GL}_2(\mathbb{Z}_2)$? If so, construct an explicit isomorphism $f : G \to \mathrm{GL}_2(\mathbb{Z}_2)$.

(Recall that a map $f : G \to H$ between groups G and H is an *isomorphism* if f is both a *homomorphism* of groups — that is, $f(xy) = f(x)f(y)$ for every $x, y \in G$ — and a bijection of sets.)

Groups G and H are said to be *isomorphic* if there exists an isomorphism $f : G \to H$. (Think about why being isomorphic is an equivalence relation on all groups!)

(2) (a) Find a subgroup of $\mathbb{Z}_{18}$ isomorphic to $\mathbb{Z}_6$. Explain.

(b) Fix $m, n \geq 1$. Find a subgroup H of $\mathbb{Z}_{mn}$ that is isomorphic to $\mathbb{Z}_n$ and constructing an explicit isomorphism $f : \mathbb{Z}_n \to H$.
(Don't forget to show that f is well defined!)

(3) Use Bézout's lemma (Judson Theorem 2.10) to prove each of the following assertions. Suppose a, b are nonzero integers with $\gcd(a, b) = 1$. Let $c \in \mathbb{Z}$ be arbitrary.

(a) If $a \mid bc$, then $a \mid c$.

(b) If $a \mid c$ and $b \mid c$, then $ab \mid c$.

Are either of the statements above still true without the assumption that $\gcd(a, b) = 1$? Prove or disprove with a counterexample.

(4) Show that $\gcd(a, n)$ only depends on the equivalence class of a modulo n. In other words, show that the map $\mathbb{Z}_n \to \mathbb{Z}^+$ sending $[a]_n$ to $\gcd(a, n)$ is well-defined.

(5) For each pair a, b below, use Euclid's algorithm to find $\gcd(a, b)$. Use your computations to find an integer solution (x, y) to $ax + by = \gcd(a, b)$. Then find a *different* integer solution.

(a) $a = 562$, $b = 471$
(b) $a = 165$, $b = 234$

(6) **Challenge problem:** Show that the relation

$$G \sim H \text{ if there exists an isomorphism } f : G \to H$$

is an equivalence relation on all groups.

(7) **Division algorithm in $\mathbb{Z}[i]$ (challenge problem):** Show that the Gaussian integers $\mathbb{Z}[i]$ has a division algorithm: that is, for every $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there exist $q, r \in \mathbb{Z}[i]$ so that

$$a = bq + r$$

with r satisfying $0 \leq N(r) < N(\beta)$.

Here the norm map, defined in HW #3 problem (8), is the function $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ given by $N(a + bi) = a^2 + b^2$. It might be helpful to show that the norm map is multiplicative.

(For ideas, you could start by reading the proof of division algorithm in $\mathbb{Z}$ (Judson Theorem 2.9). Alternatively, you could try for a geometric argument by plotting the lattice of multiples of β in $\mathbb{Z}[i]$ and tracking how far α can be from a lattice point.)