MA 541: Modern Algebra I / Fall 2019
Homework assignment # 3
Due 9/24/2019

(0) Read F section 0.

(1) Recall that for $a, b \in \mathbb{Z}$ we say that $a|b$ (read as "a divides b") if there exists a $k \in \mathbb{Z}$ such that $ak = b$.

Either prove or give a counterexample for each statement below.

(a) For all a in $\mathbb{Z}$, we have $a|a$.
(b) For all a, b, c in $\mathbb{Z}$, if $a|b$ and $b|c$, then $a|c$.
(c) For all a, b in $\mathbb{Z}$, if $a|b$ then $b|a$.
(d) For all a, b, c in $\mathbb{Z}$, if $a|b$ and $a|c$, then $a|(b + c)$.
(e) For all a, b, c in $\mathbb{Z}$, if $a|b$ and $c|b$, then $(a + c)|b$.
(f) For all a, b in $\mathbb{Z}$, if $a|b$ then $a|bc$.
(g) For all a, b in $\mathbb{Z}$, if $a|bc$ then $a|b$ and $a|c$.

(2) Solve F problems 0.29–0.32. Explain your answers!

(3) Which of the following maps are injective? Surjective? Bijective? Explain!

(a) $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2 - 1$
(b) $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3 - x$
(c) $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3$
(d) $f : \mathbb{R} - \{0\} \to \mathbb{R}$ given by $f(x) = \dfrac{1}{x}$

(4) **Units modulo n:** Fix $n \in \mathbb{Z}^+$. An element $a \in \mathbb{Z}$ is called a *unit modulo* n there exists $b \in \mathbb{Z}$ so that $ab \equiv_n 1$.

Recall that $\mathbb{Z}_n$ is the set of equivalence classes in $\mathbb{Z}$ under the $\equiv_n$ equivalence relation as discussed in class. The elements of $\mathbb{Z}_n$ are also called *residue classes* modulo n.

(a) Suppose that $a \in \mathbb{Z}$ is a unit modulo n. Prove that its inverse modulo n is well defined as a residue class in $\mathbb{Z}_n$, and depends only on the residue class $\overline{a}$ in $\mathbb{Z}_n$.
(b) Let $\mathbb{Z}_n^\times \subseteq \mathbb{Z}_n$ be the set of invertible residue classes modulo n. Prove that $\mathbb{Z}_n^\times$ forms a group under multiplication. Is this group a subgroup of $\mathbb{Z}_n$?
(c) List the elements of $\mathbb{Z}_9^\times$. How many are there? For each residue class $u \in \mathbb{Z}_9$, compute the elements of the sequence $u, u^2, u^3, u^4, \ldots$ until the pattern is clear. Determine the length of each repeating cycle. Is $\mathbb{Z}_9^\times$ a cyclic group?

(5) Is $\mathbb{Z}_7^\times$ a cyclic group? If so, find all the generators.
Same for $\mathbb{Z}_8^\times$, $\mathbb{Z}_{10}^\times$, $\mathbb{Z}_{11}^\times$, and $\mathbb{Z}_{12}^\times$.

(6) Let G and H be groups, and let $\varphi : G \to H$ be a group homomorphism. Prove that for all $g \in G$ we have

$$\varphi(g^{-1}) = \varphi(g)^{-1}.$$

(Note that the inverse on the on the left-hand side of the equality is being taken in G, and the inverse on the right-hand side in H.)

(7) **Direct product of groups:** Let $(G, *_G)$ and $(H, *_H)$ be groups, with identity elements e_G and e_H, respectively. Let g be any element of G, and h any element of H.

(a) Show that the set $G \times H$ has a natural group structure under the operation $(*_G, *_H)$. What is the identity element of $G \times H$ with this structure? What is the inverse of the element $(g, h) \in G \times H$?

(b) Show that the map $i_G : G \to G \times H$ given by $i_G(g) = (g, e_H)$ is a group homomorphism. Is it injective? Surjective? Do the same for the map $i_H : H \to G \times H$ given by $i_H(h) = (e_G, h)$.

(c) Show that the map $\pi_G : G \times H \to G$ given by $\pi_G\big((g, h)\big) = g$ is a group homomorphism. Is it injective? Surjective? Do the same for the map $\pi_H : G \times H \to H$ given by $\pi_H\big((g, h)\big) = h$.

(d) Prove that the image of i_G is the kernel of π_H, and that the image of i_H is the kernel of π_G.