Homework 1

Danny Rorabaugh and Heather Smith

Problem 1 (Golan 12). For a field $\mathbb{F} = \langle F, +, \cdot, -, 0, 1 \rangle$, show that the function $a \mapsto a^{-1}$ is a permutation of the set $F \setminus \{0_F\}$.

Solution. In order to show that $f: F \setminus \{0_F\} \to F \setminus \{0_F\}$, $f(a) = a^{-1}$ is a permutation, we prove that f is a well-defined bijection.

Well-defined: For each $a \in F \setminus \{0_F\}$, there is an element $x \in F \setminus \{0_F\}$ such that ax = xa = 1 because F is a field. In other words, $x = a^{-1}$. Now suppose there exists $y \in F \setminus \{0_F\}$ such that ay = ya = 1. Then y = 1y = xay = x1 = xax = 1x = x. Therefore inverses in F are unique.

Surjective: For any $b \in F \setminus \{0_F\}$, we have $f(b) = b^{-1} \in F \setminus \{0_f\}$ because F is a field. Observe that $bb^{-1} = b^{-1}b = 1$. Therefore, b is the unique inverse of b^{-1} . So $f(b^{-1}) = b$.

Injective: For any $a, b \in F \setminus \{0_F\}$, suppose f(a) = c = f(b) for some $c \in F \setminus \{0_F\}$. Then ac = 1 = bc, so $a = a1 = acc^{-1} = 1c^{-1} = bcc^{-1} = b1 = b$.

[Note: "If $c \neq 0$, then ac = bc implies a = b" is a general property of integral domains. You can alternatively use the fact that every field is an integral domain to prove that f is well-defined and injective.]

Problem 2 (Golan 16). Let z_1 , z_2 , and z_3 be complex numbers satisfying $|z_i| = 1$ for i = 1, 2, 3. Show that $|z_1z_2 + z_1z_3 + z_2z_3| = |z_1 + z_2 + z_3|$.

Solution. For each $j \in [3]$, since $|z_i| = 1$, note that for some real θ_j ,

$$\frac{1}{z_j} = \frac{1}{e^{i\theta_j}} = e^{-i\theta_j} = \overline{z_j}.$$

Therefore,

$$|z_1 z_2 + z_1 z_3 + z_2 z_3| = |z_1| \cdot |z_2| \cdot |z_3| \cdot \left| \frac{1}{z_3} + \frac{1}{z_2} + \frac{1}{z_1} \right|$$

$$= 1 \cdot 1 \cdot 1 \cdot |\overline{z_3} + \overline{z_2} + \overline{z_1}|$$

$$= |\overline{z_1 + z_2 + z_3}|$$

$$= |z_1 + z_2 + z_3|.$$

Problem 3 (Golan 22 Abel's inequality). Let z_1, \ldots, z_n be a list of complex numbers and, for each $1 \le k \le n$, let $s_k = \sum_{i=1}^k z_i$. For real numbers a_1, \ldots, a_n satisfying $a_1 \ge a_2 \ge \cdots \ge a_n \ge 0$, show that

$$\left| \sum_{i=1}^{n} a_i z_i \right| \le a_1 \left(\max_{1 \le k \le n} |s_k| \right). \tag{1}$$

Solution. Define $s_0 := 0$. Observe $a_i z_i = a_i s_i - a_i s_{i-1}$ for $1 \le i \le n$. Therefore

$$\begin{split} \left| \sum_{i=1}^{n} a_{i} z_{i} \right| &= \left| \sum_{i=1}^{n} a_{i} s_{i} - a_{i} s_{i-1} \right| \\ &= \left| \sum_{i=1}^{n-1} s_{i} (a_{i} - a_{i+1}) + s_{n} a_{n} \right| \\ &\leq \sum_{i=1}^{n-1} \left| s_{i} (a_{i} - a_{i+1}) \right| + \left| s_{n} a_{n} \right| & \text{by the Triangle Inequality} \\ &= \sum_{i=1}^{n-1} \left(a_{i} - a_{i+1} \right) \left| s_{i} \right| + a_{n} \left| s_{n} \right| \\ &\leq \sum_{i=1}^{n-1} \left(a_{i} - a_{i+1} \right) \max_{1 \leq k \leq n} \left| s_{k} \right| + a_{n} \max_{1 \leq k \leq n} \left| s_{k} \right| \\ &= \left(\sum_{i=1}^{n-1} (a_{i} - a_{i+1}) + a_{n} \right) \max_{1 \leq k \leq n} \left| s_{k} \right| \\ &= a_{1} \max_{1 \leq k \leq n} \left| s_{k} \right|. & \text{by telescoping sums} \end{split}$$

Problem 4 (Golan 24). If p is a prime positive integer, find all subfields of GF(p).

Solution. Since every field is a unital ring, every subfield of GF(p) contains the unit 1. The order of 1 is p, since $\underbrace{1+1+\cdots+1}_{p}=0$, but $\underbrace{1+1+\cdots+1}_{k}\neq 0$ for positive k< p.

Suppose $\underbrace{1+1+\cdots+1}_{a} = \underbrace{1+1+\cdots+1}_{b}$ for some positive a,b < p. Then a = b. Thus,

any subfield with 1 contains at least p distinct elements. Since |GF(p)| = p, it is itself the only subfield.

Problem 5. Write down the definition of a module as a (universal) algebra, $\mathbf{M} = \langle M, F \rangle$. That is, describe the set F of operations and give the conditions that they should satisfy in order for \mathbf{M} to agree with the classical definition of a module over a ring.

[Hint: Let $\mathbf{R} = \langle R, +, \cdot, -, 0, 1 \rangle$ be a ring and, for each $r \in R$, define a scalar multiply operation $f_r \in F$.]

Solution. Let $\mathbf{A} = \langle V, +, -, 0 \rangle$ be an Abelian group. Let \mathbf{R} be the unital ring

$$\mathbf{R} = \langle R, +, \cdot, -, 0, 1 \rangle$$

Define module V as follows:

$$\mathbf{V} = \langle V, +, -, 0, \{ f_r : r \in R \} \rangle$$

where the addition, additive inverse, and zero are defined on V as they are in the Abelian group **A**. Each f_r is a function $f_r: V \to V$ so that for any $r, r_1, r_2 \in R$ and any $v, v_1, v_2 \in V$ each of the following is satisfied:

- $f_r(v_1 + v_2) = f_r(v_1) + f_r(v_2)$
- $f_{r_1+r_2}(v) = f_{r_1}(v) + f_{r_2}(v)$
- $f_{r_1}(f_{r_2}(v)) = f_{r_1r_2}(v)$
- $f_1(v) = v$

Problem 6. Let $\mathbf{R} = \langle R, +, -, \cdot, 0, 1 \rangle$ be a ring.

- 1. Define left ideal of \mathbf{R} .
- 2. Let $\mathscr{A} = \{A_i : i \in \mathscr{I}\}\$ be a family of left ideals of **R**. Prove that $\bigcap \mathscr{A}$ is a left ideal.

Solution.

- 1. A left ideal I of \mathbf{R} is a subset of R which forms a subgroup under addition and for any $a \in I$ and $r \in R$, we have $ra \in I$.
- 2. Clearly $\bigcap \mathscr{A}$ is a subset of R since each $A_i \in \mathscr{A}$ is a subset of R. Let $a, b \in \bigcap \mathscr{A}$ and $r \in R$. By definition of intersection, $a, b \in A_i$ for all $A_i \in \mathscr{A}$. Therefore $ra, a + b \in A_i$ for all $A_i \in \mathscr{A}$ because each A_i is a left ideal. But this implies that $ra, a + b \in \bigcap \mathscr{A}$, proving that $\bigcap \mathscr{A}$ is a left ideal.

Problem 7. Let **R** be a ring and fix $a, b \in R$. Prove that if 1 - ba is left invertible, then 1 - ab is also left invertible. What is the inverse?

[Hint: Consider the left ideal R(1-ab). It contains the left ideal Rb(1-ab) = Rb and therefore contains 1. Verify these statements, then try to compute the inverse of 1-ab. (Ask for more hints as needed.)]

Solution. We can show existence as follows: Observe $Rb(1-ab) \subseteq R(1-ab)$ since $Rb \subseteq R$. Because (1-ba) is left invertible, R = R(1-ba) and

$$Rb = R(1 - ba)b = R(b - bab) = Rb(1 - ab).$$

Therefore $Rb \subseteq R(1-ab)$. Observe $ab \in Rb$ and $(1-ab) \in R(1-ab)$ so

$$1 = (1 - ab) + ab \in R(1 - ab),$$

which implies that (1 - ab) is invertible.

To explicitly find the left inverse of (1-ab), let $c \in R$ be such that c(1-ba) = 1. Then

$$1 = 1 - ab + ab$$

$$= 1 - ab + a1b$$

$$= 1 - ab + ac(1 - ba)b$$

$$= (1 - ab) + ac(b - bab)$$

$$= 1(1 - ab) + acb(1 - ab)$$

$$= (1 + acb)(1 - ab)$$

Therefore, the left inverse of (1-ab) is (1+acb), where c is the left inverse of (1-ba).