ALGEBRA I HOMEWORK VI

HOJIN LEE 2021–11045

Problem 1. *Solve the following.*

(1) *Show that every finite domain is a field.*
(2) *Show that if F is a finite field then $|F| = p^n$ for some prime $p > 0$ and $n \in \mathbb{N}_{\geq 1}$.*
(3) *Give an example of a ring A and element $x \in A$ that is left regular but not right regular.*

Proof. (1) Suppose D is a finite domain. Suppose $0, 1 \neq a \in D$. Consider the elements $a, a^2, a^3, \ldots$, and by the pigeonhole principle, we must have $a^i = a^j$ for some $i < j$. Then $a^i - a^j = a^i(1 - a^{j-i}) = 0$, where $a^i \neq 0$ (otherwise, a would be a zerodivisor) so we must have $a^{j-i} = 1$. Since we assumed $a \neq 1$, we have $j - i > 1$, so a has a unique multiplicative inverse. □

Proof. (2) Suppose F is a finite field. Then $\operatorname{char} F = 0$ cannot happen by finiteness of F, and $\operatorname{char} F = p$ for some prime. To show this, suppose $\operatorname{char} F = n = p_1^{n_1} \cdots p_k^{n_k}$ for some composite n. This implies $1 \cdot n = (1 \cdot p_1)^{n_1} \cdots (1 \cdot p_k)^{n_k} = 0$, and since F is a field we must have $1 \cdot p_i = 0$ for some $1 \leq i \leq k$, a contradiction since $p_i < n$. Thus, suppose $\operatorname{char} F = p$ for some prime p. The subfield generated by 1 is isomorphic to $\mathbb{F}_p$, and we may view this as a field extension $F/\mathbb{F}_p$. Thus F is a $\mathbb{F}_p$-vector space, which is finite dimensional since F is finite. Hence it is isomorphic to a finite direct sum $\bigoplus \mathbb{F}_p$, thus of order p^n for some $n \geq 1$. □

Proof. (3) Such ring should be necessarily noncommutative. Consider the ring of endomorphisms of $\mathbb{R}[x]$ as an $\mathbb{R}$-vector space. Let $T : f \mapsto fx$. If $U : 1 \mapsto 1, x^i \mapsto 0$ for $i > 0$, then $U \circ T = 0$ but if $V \neq 0$ then we have $T \circ V \neq 0$. Thus T is not right regular, but is left regular. □

Problem 2. $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ *is a ring generated over* $\mathbb{R}$.

(1) *Show that $\mathbb{H}$ is a division ring.*
(2) *Show that the center of $\mathbb{H}$ is $\mathbb{R}$.*

Proof. (1) Suppose $a = r_1 + r_2 i + r_3 j + r_4 k$ for $r_i \in \mathbb{R}$, $a \neq 0$. We show that there exists a^{-1} such that $aa^{-1} = a^{-1}a = 1$. If we let $b = r_1 - r_2 i - r_3 j - r_4 k$, then we have $ab = r_1^2 + r_2^2 + r_3^2 + r_4^2$, so if we let $a^{-1} = b/(r_1^2 + r_2^2 + r_3^2 + r_4^2)$ then we have $aa^{-1} = 1$. For the other way, we calculate ba. Note that this is just $(r_1 - r_2 i - r_3 j - r_4 k)(r_1 + r_2 i + r_3 j + r_4 k)$, so this will be $r_1^2 + (-r_2)^2 + (-r_3)^2 + (-r_4)^2$, just the same. Thus $a^{-1}a = 1$ too. Hence $\mathbb{H}$ is a division ring. □

Proof. (2) Since $ij = -ji$, i and j are not in the center. Similarly, k is not in the center. Thus the center is contained in $\mathbb{R}$. Every element of $\mathbb{R}$ commutes with other elements of $\mathbb{H}$, so the center is $\mathbb{R}$. □

Date: April 12, 2024.

Problem 3.

Problem 4.

Problem 5. *Let A be a commutative ring. Let I be an ideal of A.*

(1) *Show that $\sqrt{I}$ is an ideal, and that $\sqrt{I}$ contains I.*
(2) *Show that $\sqrt{I} = A$ iff $I = A$.*

Proof. (1) Suppose $x, y \in \sqrt{I}$. Then we have $x^n, y^m \in I$ for some $n, m > 0$. It follows that $(x+y)^{n+m} \in I$, so $x + y \in \sqrt{I}$. Obviously $0 \in \sqrt{I}$ so $\sqrt{I}$ is an additive subgroup of A. Now if we have $x \in \sqrt{I}$, say $x^n \in I$, then $(rx)^n = r^n x^n \in I$, so $rx \in \sqrt{I}$. Hence $\sqrt{I}$ is an ideal. Obviously $\sqrt{I}$ contains I since $i^1 \in I$ for all $i \in I$. $\square$

Proof. (2) $\sqrt{I} = A \Rightarrow 1 \in \sqrt{I} \Rightarrow 1 \in I$. The converse is obvious. $\square$

Problem 6. *Let A a ring. Let M an A-module, and $N, P \leq M$ are A-submodules.*

(1) *Construct the SES*
$$0 \to M/(N \cap P) \to M/N \times M/P \to M/(N+P) \to 0.$$
(2) *For $N + P = M$ conclude we have a natural isomorphism of A-modules*
$$M/(N \cap P) \cong M/N \times M/P.$$

Proof. (1) Note that we have an exact sequence
$$0 \to N \cap P \to N \times P \to N + P \to 0$$
given by $x \mapsto (x, -x)$ and $(a, b) \mapsto a + b$. One may check exactness almost trivially. Now consider the following diagram in Mod_A

$$\begin{tikzcd}
{} \arrow[r, dashed] & \operatorname{coker}\alpha \arrow[r] & \operatorname{coker}\beta \arrow[r] & \operatorname{coker}\gamma \arrow[r] & 0 \\
0 \arrow[r] & M \arrow[r] \arrow[u] & M \times M \arrow[r] \arrow[u] & M \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & N \cap P \arrow[r] \arrow[u, hook, "\alpha"] & N \times P \arrow[r] \arrow[u, hook, "\beta"] & N + P \arrow[r] \arrow[u, hook, "\gamma"] & 0 \\
 & & & 0 \arrow[u] \arrow[r, dashed, dash] & {}
\end{tikzcd}$$

where β is termwise inclusion, and the maps $M \to M \times M$ and $M \times M \to M$ are given by extending the maps on the bottom row. The diagram commutes, and the desired SES is given by the Snake lemma. $\square$

Proof. (2) Suppose $N + P = M$. Then in the SES above, we have $M/(N \cap P) \cong M/N \times M/P$. $\square$

Problem 7.