MTH 562/662 **Spring 2024**
Exam 1 **Fri Mar 8**

Convention: All rings in this exam are commutative.

Problem 1. Ring Homomorphisms.

(a) Define ring homomorphism.

Let R and S be rings. A function $\varphi : R \to S$ is called a *ring homomorphism* when it satisfies the following three properties:

- $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$,
- $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$,
- $\varphi(1) = 1$.

(b) Prove that kernel of a ring homomorphism is an ideal.

An *ideal* is an additive subgroup $I \subseteq (R, +, 0)$ satisfying the extra property that $ab \in I$ for all $a \in R$ and $b \in I$. Equivalently, an ideal is a subset $I \subseteq R$ satisfying $a + bc \in I$ for all $a, b \in I$ and $c \in R$. If $\varphi : R \to S$ is a ring homomorphism we define the kernel

$$\ker \varphi := \{a \in R : \varphi(a) = 0\}.$$

This is an ideal of R since for $a, b \in \ker \varphi$ and $c \in R$ we have

$$\varphi(a + bc) = \varphi(a) + \varphi(b)\varphi(c) = 0 + 0c = 0,$$

and hence $a + bc \in \ker \varphi$.

(c) Prove that image of a ring homomorphism is a subring.

A *subring* of S is a subset $T \subseteq S$ satisfying the following properties:

- $0 \in T$ and $1 \in T$,
- for all $a, b \in T$ we have $a + b \in T$ and $ab \in T$.

Given a ring homomorphism $\varphi : R \to S$ we define the *image*

$$\operatorname{im} \varphi := \{\varphi(a) : a \in R\}.$$

This is a subring of S since $0 = \varphi(0) \in \operatorname{im} \varphi$,[1] $1 = \varphi(1) \in \operatorname{im} \varphi$, and for any $\varphi(a), \varphi(b) \in \operatorname{im} \varphi$ we have

$$\varphi(a) + \varphi(b) = \varphi(a+b) \in \operatorname{im} \varphi \quad \text{and} \quad \varphi(a)\varphi(b) = \varphi(ab) \in \operatorname{im} \varphi.$$

Problem 2. Fields.

(a) Let $I \subseteq R$ be an ideal of a ring. Prove that $I = R$ if and only if I contains a unit.

First suppose that $I = R$. Then I contains a unit because $1 \in I$. Conversely, suppose that I contains a unit $u \in R^\times$. Then for any $a \in R$ we have $a = (au^{-1})u \in I$ because $au^{-1} \in R$ and $u \in I$. Hence $I = R$.

---

[1] The fact that $\varphi(0) = 0$ follows from the property $\varphi(a+b) = \varphi(a) + \varphi(b)$ and the fact that φ is a homomorphism of additive groups.

(b) Let R be a ring. Prove that R is a field if and only if it has exactly two ideals.

Any ring R has the ideals $\{0\}$ and R. We will show that R is a field if and only if these are its only ideals. First suppose that R is a field and let $I \subseteq R$ be any ideal. If $I \neq \{0\}$ then there exists a nonzero element $a \in I$. But every nonzero element of a field is a unit, hence it follows from part (a) that $I = R$. Conversely, let R be a ring and suppose that $\{0\}$ and R are its only ideals. Let $a \in R$ be any nonzero element and consider the ideal $aR \subseteq R$. Since $a \in aR$ and $a \neq 0$ we have $aR \neq \{0\}$, and hence $aR = R$. Then since $1 \in aR$ it follows that $1 = ab$ for some $b \in R$. Hence R is a field.

Problem 3. Minimal Polynomials. Let $\mathbb{E} \supseteq \mathbb{F}$ be a field extension and let $\alpha \in \mathbb{E}$ be any element. Then we have a ring homomorphism $\varphi_\alpha : \mathbb{F}[x] \to \mathbb{E}$ defined by $f(x) \mapsto f(\alpha)$.

(a) Define $\mathbb{F}[\alpha] := \operatorname{im} \varphi_\alpha$. Prove that $\mathbb{F}[\alpha]$ is the smallest subring of $\mathbb{E}$ that contains $\mathbb{F} \cup \{\alpha\}$.

From Problem 1(c) we know that $\mathbb{F}[\alpha]$ is a subring of $\mathbb{E}$. Now let $R \subseteq \mathbb{E}$ be any subring that contains the set $\mathbb{F} \cup \{\alpha\}$. We will show that R contains $\mathbb{F}[\alpha]$. Indeed, every element of $\mathbb{F}[\alpha]$ has the form $f(\alpha)$ for some polynomial $f(x) = a_0 + \cdots + a_n x^n$ with $a_0, \ldots, a_n \in \mathbb{F}$. Since $\alpha, a_0, \ldots, a_n \in R$ and since R is closed under addition and multiplication, we have

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in R.$$

(b) You may assume that $\ker \varphi_\alpha = m_\alpha(x)\mathbb{F}[x]$ for some monic polynomial $m_\alpha(x) \in \mathbb{F}[x]$. Prove that $m_\alpha(x)$ is irreducible over $\mathbb{F}$.

For any $f(x) \in \mathbb{F}[x]$ we have $f(\alpha) = 0$ (i.e., $f(x) \in \ker \varphi_\alpha$) if and only $m_\alpha(x)|f(x)$ in the ring $\mathbb{F}[x]$. I claim that $m_\alpha(x)$ is irreducible over $\mathbb{F}$. To prove this, suppose for contradiction that we have $m_\alpha(x) = f(x)g(x)$ with $f(x), g(x) \in \mathbb{F}[x]$ and $\deg(f), \deg(g) < \deg(m_\alpha)$. Substituting $x = \alpha$ gives $0 = m_\alpha(\alpha) = f(\alpha)g(\alpha)$, which implies that $f(\alpha) = 0$ or $g(\alpha) = 0$. Without loss, suppose that $f(\alpha) = 0$, so that $m_\alpha(x)$ divides $f(x)$. But then we have $\deg(m_\alpha) \leq \deg(f) < \deg(m_\alpha)$.

(c) Suppose that $\deg(m_\alpha) = n$. In this case, prove that every element $\beta \in \mathbb{F}[\alpha]$ can be written in the form $\beta = a_0 + a_1\alpha + a_{n-1}\alpha^{n-1}$ for some $a_0, \ldots, a_{n-1} \in \mathbb{F}$.

Every element $\beta \in \mathbb{F}[\alpha]$ has the form $\beta = f(\alpha)$ for some $f(x) \in \mathbb{F}[x]$. Divide $f(x)$ by the nonzero polynomial $m_\alpha(x)$ to obtain $q(x), r(x) \in \mathbb{F}[x]$ satisfying

$$\begin{cases} f(x) = m_\alpha(x)q(x) + r(x), \\ r(x) = 0 \text{ or } \deg(r) < n. \end{cases}$$

Since $r(x) = 0$ or $\deg(r) < n$ we can write $r(x) = a_0 + \cdots + a_{n-1}x^{n-1}$ for some $a_0, \ldots, a_{n-1} \in \mathbb{F}$. But then we have

$$\begin{aligned} \beta &= f(\alpha) \\ &= m_\alpha(\alpha)q(\alpha) + r(\alpha) \\ &= 0q(\alpha) + r(\alpha) \\ &= r(\alpha) \\ &= a_0 + a_1\alpha + a_{n-1}\alpha^{n-1}, \end{aligned}$$

as desired.

(d) Continuing from (c), consider any $f(x), g(x) \in \mathbb{F}[x]$ with $\deg(f), \deg(g) < n$. In this case, prove that $f(\alpha) = g(\alpha)$ in $\mathbb{E}$ if and only if $f(x) = g(x)$ in $\mathbb{F}[x]$.

Consider any polynomials $f(x), g(x) \in \mathbb{F}[x]$ with $\deg(f), \deg(g) < n$. If $f(x) = g(x)$ then clearly $f(\alpha) = g(\alpha)$. Conversely, suppose that $f(\alpha) = g(\alpha)$, and define the polynomial $h(x) = f(x) - g(x)$. Since $h(\alpha) = f(\alpha) - g(\alpha) = 0$ we see that $m_\alpha(x)|h(x)$ in the ring $\mathbb{F}[x]$. If $h(x)$ is not the zero polynomial then we obtain the contradiction

$$n = \deg(m_\alpha) \leq \deg(h) = \deg(f - g) \leq \max\{\deg(f), \deg(g)\} < n.$$

It follows that $h(x) = 0$, and hence $f(x) = g(x)$, in the ring $\mathbb{F}[x]$.