Math 562/662 **Exam 3**
Spring 2022 **Mon May 2**

No electronic devices are allowed. There are 4 pages. Each page worth 6 points, for a total of 24 points.

Problem 1. Finish each statement.

(a) A subset $I \subseteq R$ of a ring is called an *ideal* when...

- $0 \in I$,
- $(I, +, 0)$ is a subgroup of $(R, +, 0)$,
- $a \in I$ and $b \in R$ imply $ab \in I$.

Alternatively: For all $a, b \in I$ and $c \in R$ we have $a - bc \in I$.

(b) A function $\varphi : R \to S$ between rings is called a *ring homomorphism* when...

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

(c) The *kernel* and *image* of a ring homomorphism $\varphi : R \to S$ are defined as follows...

$$\ker \varphi = \{a \in R : \varphi(a) = 0\},$$
$$\operatorname{im} \varphi = \{b \in S : \exists a \in R, \varphi(a) = b\}.$$

Problem 2.

(a) Let $I \subseteq R$ be an ideal. Prove that the following operation on cosets is well-defined:

$$(a + I)(b + I) := ab + I.$$

Proof. Assume that $a + I = a' + I$ and $b + I = b' + I$, so that $a - a' \in I$ and $b - b' \in I$. Then since I is an ideal we have

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I,$$

so that $ab + I = a'b' + I$. □

(b) Let R be an integral domain. For all $a, b \in R$ prove that

$$aR = bR \iff au = b \text{ for some unit } u \in R^\times.$$

Proof. First suppose that $au = b$ for some $u \in R^\times$. Then for any $r \in R$ we have $br = (au)r = a(ur) \in aR$, so that $bR \subseteq aR$. Since u^{-1} exists we also have $b = au^{-1}$ so for any $r \in R$ we have $br = a(u^{-1}r) \in aR$ and hence $bR \subseteq aR$.

Conversely, suppose that $aR = bR$. We want to show that $au = b$ for some $u \in R^\times$. If $a = 0$ or $b = 0$ then we can take $u = 1$. So let us assume that $a \neq 0$ and $b \neq 0$. By assumption we have $a = a1 \in aR = bR$ and $b = b1 \in bR = aR$, so that $a = bv$

and $b = au$ for some $u, v \in R$. We will show that $u, v \in R^\times$. Indeed, since R is a domain and $a \neq 0$ we have

$$\begin{aligned} a &= bv \\ a &= auv \\ a(1 - uv) &= 0 \\ 1 - uv &= 0 \\ 1 &= uv. \end{aligned}$$

□

Problem 3. Let $\alpha \in \mathbb{E} \supseteq \mathbb{F}$ be an element of a field extension and consider the ring homomorphism defined by evaluation:

$$\begin{array}{rccc} \varphi : & \mathbb{F}[x] & \to & \mathbb{E} \\ & f(x) & \mapsto & f(\alpha). \end{array}$$

Suppose that $\ker \varphi = m(x)\mathbb{F}[x]$, where $m(x)$ is monic and non-constant.

(a) Prove that the polynomial $m(x)$ is irreducible over $\mathbb{F}$.

Proof. Let $m(x) = f(x)g(x)$ for some $f(x), g(x) \in \mathbb{F}[x]$. Our goal is to show that $f(x)$ or $g(x)$ is constant.[1] Since $m(x) \in \ker \varphi$ we have $m(\alpha) = 0$ and hence

$$0 = m(\alpha) = f(\alpha)g(\alpha).$$

This implies that $f(\alpha) = 0$ or $g(\alpha) = 0$; let's say $f(\alpha) = 0$. But now we have $f(x) \in \ker \varphi = m(x)\mathbb{F}[x]$ and hence $f(x) = m(x)h(x)$ for some $h(x) \in \mathbb{F}[x]$. Since $\mathbb{F}[x]$ is a domain and $f(x) \neq 0$ this implies that

$$\begin{aligned} f(x) &= m(x)h(x) \\ f(x) &= f(x)g(x)h(x) \\ f(x)(1 - g(x)h(x)) &= 0 \\ 1 - g(x)h(x) &= 0 \\ 1 &= g(x)h(x), \end{aligned}$$

and hence $g(x)$ is constant. □

(b) Let $f(x) \in \mathbb{F}[x]$ be any monic irreducible polynomial satisfying $f(\alpha) = 0$. Prove that we must have $f(x) = m(x)$.

Proof. If $f(\alpha) = 0$ then we have $f(x) \in \ker \varphi = m(x)\mathbb{F}[x]$, so that $m(x)|f(x)$. If $f(x)$ is irreducible then since $m(x)$ is non-constant we have $f(x) = \lambda m(x)$ for some constant λ. Finally, since $f(x)$ and $m(x)$ are both monic we have $\lambda = 1$. □

Problem 4.

---

[1] Equivalently, either $f(x)$ or $g(x)$ is associate to $m(x)$.

(a) Consider a polynomial $f(x) \in \mathbb{F}[x]$ of degree 3. If $f(x)$ is **reducible** over $\mathbb{F}$, prove that $f(x)$ has a root in $\mathbb{F}$.

Proof. Let $f(x) \in \mathbb{F}[x]$ be reducible, so that $f(x) = g(x)h(x)$ for some non-constant $g(x), h(x) \in \mathbb{F}[x]$. Comparing degrees gives

$$3 = \deg(f) = \deg(g) + \deg(h).$$

Since $g(x)$ and $h(x)$ are non-constant we must have $\deg(g), \deg(h) \geq 1$, so the above equality implies that $\deg(g) = 1$ or $\deg(h) = 1$. Let's say $\deg(g) = 1$, so that $g(x) = ax + b$ for some $a, b \in \mathbb{F}$ with $a \neq 0$. It follows that

$$f(-b/a) = g(-b/a)h(-b/a) = 0 \cdot h(-b/a) = 0,$$

so that $-b/a \in \mathbb{F}$ is a root of $f(x)$. □

(b) Let $\mathbb{F}_3 = \{0, 1, 2\}$ be the field with three elements. Use part (a) to prove that the polynomial $x^3 + 2x + 1$ is irreducible over $\mathbb{F}_3$.

Proof. By part (a) it is sufficient to check that $x^3 + 2x + 1$ has no root in $\mathbb{F}_3$, and this is easy because $\mathbb{F}_3$ has only three elements:[2]

x	0	1	2
$x^3 + 2x + 1$	1	1	1

Bonus (Continued from 4b). Since $x^3 + 2x + 1$ is irreducible over $\mathbb{F}_3$ we know that the following quotient ring is a field:

$$\mathbb{E} = \mathbb{F}_3[x]/(x^3 + 2x + 1)\mathbb{F}_3[x].$$

Compute the inverse of the element

$$\alpha := x + (x^3 + 2x + 1)\mathbb{F}_3[x] \in \mathbb{E}.$$

Solution. For any polynomial $f(x) \in \mathbb{F}_3[x]$ we have

$$f(\alpha) = f(x) + (x^3 + 2x + 1)\mathbb{F}_3[x].$$

This shows that $\mathbb{E} = \mathbb{F}_3[\alpha]$. It also shows that $\alpha^3 + 2\alpha + 1 = 0 \in \mathbb{E}$, which since $x^3 + 2x + 1$ is irreducible over $\mathbb{F}_3[x]$ implies that

$$m_{\alpha/\mathbb{F}_3}(x) = x^3 + 2x + 1.$$

Finally, since $\deg(m_{\alpha/\mathbb{F}_3}) = 3$ we know from the Minimal Polynomial Theorem that every element of $\mathbb{E}$ can be expressed as $a + b\alpha + c\alpha^2$ for **unique** $a, b, c \in \mathbb{F}_3$. Our goal is to find $a, b, c \in \mathbb{F}_3$ such that

$$\begin{aligned} 1 + 0\alpha + 0\alpha^2 &= \alpha(a + b\alpha + c\alpha^2) \\ &= a\alpha + b\alpha^2 + c\alpha^3 \\ &= a\alpha + b\alpha^2 + c(-1 - 2\alpha) \\ &= -c + (a - 2c)\alpha + b\alpha^2. \end{aligned}$$

By uniqueness we may equate coefficients to get $-c = 1$, $a - 2c = 0$ and $b = 0$. It follows that $(a, b, c) = (-2, 0, -1) = (1, 0, 2)$,[2] and hence $\alpha^{-1} = 1 + 2\alpha^2$. □

[2] Don't forget, we are working mod 3.