Math 562/662 **Spring 2024**
Homework 3 **Drew Armstrong**

---

1. One Step Ideal Test. Let I be a subset of a commutative ring $(R, +, \cdot, 0, 1)$. We say that I is an *ideal of* R when the following two properties hold:

(1) I is a subgroup of $(R, +, 0)$.
(2) For all $a \in R$ and $b \in I$ we have $ab \in I$.

Prove that these two properties are equivalent to the following single property:

(3) For all $a, b \in I$ and $c \in R$ we have $a + bc \in I$.

[Hint: You may use the One Step Subgroup Test from last semester.]

Suppose that (1) and (2) hold. Then for any $a, b \in I$ and $c \in R$ we have $bc \in I$ by (2) and then $a + bc \in I$ by (1). Hence (3) holds. Conversely, suppose that (3) holds. We will use the One Step Subgroup Test to prove (1). So consider any $a, b \in I$. Then by taking $c = -1$ we have $a - b = a + bc \in I$, as desired. In particular we have $0 \in I$. Now taking $a = 0$ in the statement of (3) says that $b \in I$ and $c \in R$ imply $bc = 0 + bc \in I$, hence (2) holds.

2. First Isomorphism Theorem for Rings. Let $\varphi : R \to S$ be a ring homomorphism. We define the *image* and *kernel* as follows:

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

(a) Prove that $\ker\varphi \subseteq R$ is an ideal.
(b) Prove that $\operatorname{im}\varphi \subseteq S$ is a *subring* (i.e., a subset containing 0 and 1 that is closed under addition and multiplication).
(c) From last semester we know that the function $\Phi : R/\ker\varphi \to \operatorname{im}\varphi$ defined by $[a] \mapsto \varphi(a)$ is an isomorphism of additive groups. Prove that Φ also preserves multiplication, hence it gives a **ring isomorphism** $R/\ker\varphi \cong \operatorname{im}\varphi$.

(a): We will use the One Step Ideal Test. For any $a, b \in \ker\varphi$ and $b \in R$ we have

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

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

(b): First note that $\operatorname{im}\varphi$ contains 0 and 1 because $0 = \varphi(0)$ and $1 = \varphi(1)$. Now consider any two elements $a, b \in \operatorname{im}\varphi$. By definition, this means that $a = \varphi(a')$ and $b = \varphi(b')$ for some $a', b' \in R$. But then we have $a + b = \varphi(a') + \varphi(b') = \varphi(a' + b') \in \operatorname{im}\varphi$ and $ab = \varphi(a')\varphi(b') = \varphi(a'b') \in \operatorname{im}\varphi$, as desired.

(c): For any $a \in R$ let $[a]$ denote the additive coset $a + \ker\varphi$. We know from last semester that the operation $[a] + [b] := [a + b]$ is well-defined and makes $R/\ker\varphi$ into a group. Furthermore, the function $\Phi : R/\ker\varphi \to \operatorname{im}\varphi$ defined by $\Phi([a]) := \varphi(a)$ is a well-defined group isomorphism. On HW2 you showed that the operation $[a][b] := [ab]$ is well-defined and makes $R/\ker\varphi$ into a ring. Then Φ is also a ring homomorphism because $\Phi([1]) = \varphi(1) = 1$ and $\Phi([a][b]) = \Phi([ab]) = \varphi(ab) = \varphi(a)\varphi(b) = \Phi([a])\Phi([b])$. Hence Φ is a ring isomorphism $R/\ker\varphi \cong \operatorname{im}\varphi$.

3. Characteristic of a Ring. For any ring R there exists a unique ring homomorphism $\iota_R : \mathbb{Z} \to R$ from the ring of integers. Since $\ker \iota_R$ is an ideal of $\mathbb{Z}$ we must have $\ker \iota_R = n\mathbb{Z}$ for some unique natural number $n \in \mathbb{N}$. We call this the *characteristic of* R:

$$\text{char}(R) := n.$$

(a) Prove that $\text{im}\, \iota_R$ is the smallest subring of R.
(b) If R is a domain, prove that $\text{char}(R) = 0$ or $\text{char}(R) = p$ for some prime $p \geq 2$. [Hint: By the first isomorphism theorem, $\mathbb{Z}/\ker \iota_R$ is isomorphic to a subring of R.]
(c) Let $\mathbb{F}$ be a field and let $\mathbb{F}' \subseteq \mathbb{F}$ be the smallest subfield.[1] Since every field is a domain, we know from part (b) that $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) = p \geq 2$. In the first case show that $\mathbb{F}' \cong \mathbb{Q}$. In the second case show that $\mathbb{F}' \cong \mathbb{Z}/p\mathbb{Z}$. [Hint: From part (a) we know that $R := \text{im}\, \iota_{\mathbb{F}}$ is the smallest subring of $\mathbb{F}$. Show that $\text{Frac}(R) = \mathbb{F}'$ and then use the First Isomorphism Theorem.]

(a): The function ι_R can be described as $\iota_R(n) = n \cdot 1_R$ where

$$n \cdot 1_R := \begin{cases} 1_R + 1_R + \cdots + 1_R & n \geq 1, \\ 0 & n = 0, \\ -1_R - 1_R - \cdots - 1_R & n \leq -1. \end{cases}$$

This notation satisfies $(m+n)\cdot 1_R = m \cdot 1_R + n \cdot 1_R$, which shows that $\text{im}\, \iota_R$ is a subring of R. (Or just use the fact that any image is a subring.) Now let $R' \subseteq R$ be the smallest subring of R. Since $\text{im}\, \iota_R$ is a subring of R we must have $R' \subseteq \text{im}\, \iota_R$. Conversely, since $1_R \in R'$ we can show by induction that $n \cdot 1_R \in R'$ for all $n \in \mathbb{Z}$, and hence $\text{im}\, \iota_R \subseteq R'$.

(b): Let R be a domain. Since $\ker \iota_R$ is an ideal of $\mathbb{Z}$ we have $\ker \iota_R = n\mathbb{Z}$ for some unique $n \in \mathbb{N}$, and we write $n = \text{char}(R)$. I claim that $n = 0$ or $n = p$ for prime $p \geq 2$. Indeed, by the First Isomorphism Theorem we know that $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker \iota_R \cong \text{im}\, \iota_R \subseteq R$. Since $\text{im}\, \iota_R$ is a subring of a domain, it is also a domain. Then since $\mathbb{Z}/n\mathbb{Z}$ is a domain we know that $n\mathbb{Z} \subseteq \mathbb{Z}$ is a prime ideal. Hence $n = 0$ or $n = p$ for prime $p \geq 2$.

(c): Let $\mathbb{F}$ be a field with smallest subfield $\mathbb{F}' \subseteq \mathbb{F}$ and smallest subring $R' \subseteq \mathbb{F}$, so that $R' \subseteq \mathbb{F}'$. I claim that $\mathbb{F}' = \text{Frac}(R')$, where $\text{Frac}(R')$ is defined as the set $\{ab^{-1} : a, b \in R', b \neq 0\} \subseteq \mathbb{F}$. Indeed, for all $a, b \in R'$ with $b \neq 0$ we have $a, b \in \mathbb{F}'$ and hence $ab^{-1} \in \mathbb{F}'$, so that $\text{Frac}(R') \subseteq \mathbb{F}'$. Conversely, since $\text{Frac}(R')$ is a subfield of $\mathbb{F}$ and since $\mathbb{F}'$ is the smallest subfield we have $\mathbb{F}' \subseteq \text{Frac}(R')$.

Since $\mathbb{F}$ is a domain we know from (b) that $R' \cong \mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ or $R' \cong \mathbb{Z}/p\mathbb{Z}$ for prime $p \geq 2$. Hence $\mathbb{F}' \cong \text{Frac}(\mathbb{Z}) = \mathbb{Q}$ or $\mathbb{F}' \cong \text{Frac}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$.

4. Minimal Polynomials. Given an element $\alpha \in \mathbb{E} \supseteq \mathbb{F}$ of a field extension we have a ring homomorphism $\varphi_\alpha : \mathbb{F}[x] \to \mathbb{E}$ defined by $f(x) \mapsto f(\alpha)$. Since $\mathbb{F}[x]$ is Euclidean we know that $\ker \varphi_\alpha = m_\alpha(x)\mathbb{F}[x]$ for some unique monic polynomial $m_\alpha(x) \in \mathbb{F}[x]$ called the *minimal polynomial of* α *over* $\mathbb{F}$. We will assume that $m_\alpha(x) \neq 0$[2] and $\deg(m_\alpha) = n$.

(a) Prove that $m_\alpha(x)$ is irreducible over $\mathbb{F}$. [Hint: Suppose for contradiction that $m_\alpha(x) = f(x)g(x)$ with $\deg(f), \deg(g) \geq 1$. Evaluating $x \mapsto \alpha$ gives $f(\alpha)g(\alpha) = 0$ so without loss of generality we can assume that $f(\alpha) = 0$. But this implies that $f(x) \in \ker \varphi_\alpha$ so that $f(x) = m_\alpha(x)h(x)$ for some $h(x) \in \mathbb{F}[x]$.]

[1] A subfield is a subring that is also a field.
[2] That is, we will assume that α is *algebraic over* $\mathbb{F}$.

(b) Recall that we define $\mathbb{F}[\alpha] := \operatorname{im} \varphi_\alpha$. Prove that every element of $\mathbb{F}[\alpha]$ can be written in the form $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ with $a_0, \ldots, a_{n-1} \in \mathbb{F}$. [Hint: By definition every element $\beta \in \mathbb{F}[\alpha]$ has the form $\beta = f(\alpha)$ for some polynomial $f(x) \in \mathbb{F}[x]$. Divide $f(x)$ by the nonzero polynomial $m_\alpha(x)$ and then substitute $x \mapsto \alpha$.]

(c) For any $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1} \in \mathbb{F}$ prove that

$$\sum_{k=0}^{n-1} a_k \alpha^k = \sum_{k=0}^{n-1} b_k \alpha^k \quad \Longleftrightarrow \quad a_k = b_k \text{ for all } 0 \leq k \leq n-1.$$

(a): Suppose for contradiction that $m_\alpha(x) = f(x)g(x)$ for some $f(x), g(x) \in \mathbb{F}[x]$ with $\deg(f), \deg(g) \geq 1$. Since $\deg(m_\alpha) = \deg(f) + \deg(g)$ this implies that $\deg(f), \deg(g) < \deg(m_\alpha)$. Now evaluating $x \mapsto \alpha$ gives $f(\alpha)g(\alpha) = m_\alpha(\alpha) = 0$. Since $\mathbb{E}$ is a domain this implies that $f(\alpha) = 0$ or $g(\alpha) = 0$. Without loss of generality, let's say $f(\alpha) = 0$. By the definition of $m_\alpha(x)$ this means that $f(x) = m_\alpha(x)h(x)$ for some $h(x) \in \mathbb{F}[x]$. But since $f(x) \neq 0$ this implies that $\deg(f) = \deg(m_\alpha) + \deg(h) \geq \deg(m_\alpha)$, which contradicts the fact that $\deg(f) < \deg(m_\alpha)$.

(b): Let $\deg(m_\alpha) = n$ and consider any element $\beta \in \mathbb{F}[\alpha]$. By definition this means that $\beta = f(\alpha)$ for some polynomial $f(x) \in \mathbb{F}[x]$. Divide $f(x)$ by the minimal polynomial $m_\alpha(x)$ to obtain $q(x), r(x) \in \mathbb{F}[x]$ satisfying

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

In any case we can write $r(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ for some $a_0, \ldots, a_{n-1} \in \mathbb{F}$. Then evaluating $x \mapsto \alpha$ gives

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

as desired.

(c): Consider any two polynomials $f(x) = a_0 + \cdots + a_{n-1}x^{n-1}$ and $g(x) = b_0 + \cdots + b_{n-1}x^{n-1}$ in $\mathbb{F}[x]$ of degree $< n$. If $a_k = b_k$ for all k then $f(x) = g(x)$ and hence $f(\alpha) = g(\alpha)$. Conversely, suppose that $f(\alpha) = g(\alpha)$ and consider the polynomial $h(x) = f(x) - g(x) \in \mathbb{F}[x]$. Our goal is to show that $h(x) = 0$, which implies that each of its coefficients $a_k - b_k$ is zero, and hence $a_k = b_k$. So suppose for contradiction that $h(x) \neq 0$. Since $h(\alpha) = f(\alpha) - g(\alpha) = 0$ we have $h(x) = m_\alpha(x)p(x)$ for some $p(x) \in \mathbb{F}[x]$ and since $h(x) \neq 0$ this implies that $\deg(h) = \deg(m_\alpha) + \deg(p) \geq \deg(m_\alpha) = n$. But this contradicts the fact that $\deg(h) = \deg(f - g) \leq \max\{\deg(f), \deg(g)\} < n$.

5. Irreducible Polynomials of Small Degree. Let $\mathbb{F}$ be a domain and let $f(x) \in \mathbb{F}[x]$ be a polynomial of degree 2 or 3. Prove that

$$f(x) \text{ is irreducible over } \mathbb{F} \quad \Longleftrightarrow \quad f(x) \text{ has no root in } \mathbb{F}.$$

[Hint: If $f(a) = 0$ for some $a \in \mathbb{F}$ then Descartes' Factor Theorem says that $f(x) = (x-a)g(x)$ for some $g(x) \in \mathbb{F}[x]$. Conversely, suppose that $f(x) = g(x)h(x)$ for some $g(x), h(x)$ with $\deg(g), \deg(h) \geq 1$. Now what?]

Let $\deg(f) = 2$ or 3. If $f(x) \in \mathbb{F}[x]$ has a root $a \in \mathbb{F}$ then $f(x) = (x-a)g(x)$ for some $g(x) \in \mathbb{F}[x]$, which implies that $f(x)$ is not irreducible. Conversely, suppose that $f(x)$ is reducible, say $f(x) = g(x)h(x)$ for some $\deg(g), \deg(h) \geq 1$. Since $\deg(f) = 2$ or 3, this implies that $\deg(g) = 1$ or $\deg(h) = 1$. Without loss of generality, suppose that $\deg(g) = 1$ so that $g(x) = a + bx$ with $a, b \in \mathbb{F}$ and $b \neq 0$. But then

$$f(-ab^{-1}) = g(-ab^{-1})h(-ab^{-1}) = 0h(-ab^{-1}) = 0,$$

which shows that $f(x)$ has a root $-ab^{-1} \in \mathbb{F}$.

6. The Rational Root Test. Let $f(x)$ be a polynomial of degree n with integer coefficients: $c_0 + c_1x + \cdots + c_nx^n \in \mathbb{Z}[x]$ with $c_n \neq 0$.

(a) Suppose that $f(a/b) = 0$ for some integers $a, b \in \mathbb{Z}$ with $b \neq 0$ and $\gcd(a,b) = 1$. In this case prove that $a|c_0$ and $b|c_n$. [Hint: Multiply both sides of $f(a/b) = 0$ by b^n to obtain an equation involving only integers. Show that $b|c_na^n$ and $a|c_0b^n$, then use Euclid's Lemma.]

(b) Use part (a) to show that the polynomial $x^3 - 2$ has no rational roots. It follows from Problem 5 that $x^3 - 2$ is irreducible over $\mathbb{Q}$.

(c) Let $\alpha := \sqrt[3]{2}$ be the real cube root of 2. Use part (b) to prove that $x^3 - 2$ is the minimal polynomial of α over $\mathbb{Q}$. [Hint: Let $m_\alpha(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Since $(\alpha)^3 - 2 = 0$ we know that $x^3 - 2 = m_\alpha(x)f(x)$ for some $f(x) \in \mathbb{Q}[x]$.]

(a): Suppose that $f(a/b) = 0$ for some integers $a, b \in \mathbb{Z}$ with $b \neq 0$ and $\gcd(a,b) = 1$. Multiplying both sides of this equation by b^n gives

$$\begin{aligned} f(a/b) &= 0 \\ c_0 + c_1(a/b) + \cdots + c_n(a/b)^n &= 0 \\ c_0b^n + c_1ab^{n-1} + \cdots + c_na^n &= 0. \end{aligned}$$

On the one hand we have $-c_0b^n = c_1ab^{n-1} + \cdots + c_na^n = a(c_1b^{n-1} + \cdots + c_na^{n-1})$. Then since $a|c_0b^n$ and $\gcd(a,b) = 1$, Euclid's Lemma implies that $a|c_0$. On the other hand we have $-c_na^n = c_0b^n + \cdots + c_{n-1}a^{n-1}b = b(c_0b^{n-1} + \cdots + c_{n-1}a^{n-1})$. Then since $b|c_na^n$ and $\gcd(a,b) = 1$, Euclid's Lemma implies that $b|a_n$.

(b): Suppose that $(a/b)^3 - 2 = 0$ for some $a, b \in \mathbb{Z}$ with $\gcd(a,b) = 1$. From part (a) this implies that $a|2$ and $b|1$, hence $a/b = \pm 1, \pm 2$. But $(\pm 1)^3 - 2 \neq 0$ and $(\pm 2)^3 - 2 \neq 0$. Hence this polynomial has no rational roots. Since $x^3 - 2$ has degree 3, it follows from Problem 5 that $x^3 - 2$ is irreducible over $\mathbb{Q}$.

(c): Let $\alpha := \sqrt[3]{2}$ be the real cube root of 2, so that $\alpha^3 - 2 = 0$. By definition this means that $x^3 - 2 = m_\alpha(x)f(x)$ for some $f(x) \in \mathbb{Q}[x]$, where $m_\alpha(x) \in \mathbb{Q}[x]$ is the minimal polynomial of α over $\mathbb{Q}$. But we know from part (b) that $x^3 - 2$ is irreducible over $\mathbb{Q}$, hence we must have $x^3 - 2 \sim m_\alpha(x)$, and since $m_\alpha(x)$ is monic we must have $x^3 - 2 = m_\alpha(x)$.