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:

$$\text{For all } a,b\in I \text{ and } c\in R \text{ we have } a+bc\in I.$$

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

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** $R/\ker\varphi\cong\operatorname{im}\varphi$.

3. Characteristic of a Ring. For any ring R there exists a unique ring homomorphism $\iota:\mathbb{Z}\to R$ 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:

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

(a) Prove that $\operatorname{im}\iota_R$ is the smallest subring of R.
(b) If R is a domain, prove that $\operatorname{char}(R)=0$ or $\operatorname{char}(R)=p$ 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 $\operatorname{char}(\mathbb{F})=0$ or $\operatorname{char}(\mathbb{F})=p\geq 2$. 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 $R:=\operatorname{im}\iota_{\mathbb{F}}$ is the smallest subring of $\mathbb{F}$. Show that $\operatorname{Frac}(R)=\mathbb{F}'$ and then use the First Isomorphism Theorem.]

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

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

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?]

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 $f(x) \in \mathbb{Q}[x]$.]