Math 562/662 **Spring 2022**
Homework 5 **Drew Armstrong**

---

1. A Field is a Ring with Exactly Two Ideals. Let R be a commutative ring.

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

(b) If R is a field, use part (a) to show that $\{0\} \subsetneq I \subseteq R$ implies $I = R$.

(c) Conversely, suppose that R has exactly two ideals: $\{0\}$ and R. Use this to prove that R is a field. [Hint: For any non-zero element $0 \neq a \in R$, the ideal aR must equal R. Use this to prove that a^{-1} exists.]

2. Quotients of Euclidean Domains. Let (R, N) be a Euclidean domain.

(a) Show that every ideal $I \subseteq R$ has the form $I = aR$ for some $a \in R$. [Hint: If $I = \{0\}$ then we have $I = 0R$. If $I \neq \{0\}$, choose some non-zero element $a \in I$ with minimum size $N(a)$. Show that $I = aR$.]

(b) Show that $aR = bR$ if and only if a and b are associates.

(c) Consider an ideal $pR \neq R$ (so that p is not a unit). If p is prime,[1] prove that R/pR is a field. [Hint: Consider a non-zero coset $a + pR \neq 0 + pR$. Show that we must have $\gcd(a, p) = 1$, hence from Bézout's Identity we have $ax + py = 1$ for some $x, y \in R$.]

3. The Minimal Polynomial Theorem. Consider a field extension $\mathbb{E} \supseteq \mathbb{F}$. Then for any element $\alpha \in \mathbb{E}$ we have an *evaluation homomorphism*:

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

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

(b) Let α be algebraic over $\mathbb{F}$, so that $\ker \varphi_\alpha \neq \{0\}$. In this case, prove that there exists a unique monic[2] polynomial $m(x) \in \mathbb{F}[x]$ such that $\ker \varphi_\alpha = m(x)\mathbb{F}[x]$. [Hint: Use Problem 2(a,b).] This $m(x)$ is called *the minimal polynomial of* α *over* $\mathbb{F}$.

(c) Let $d = \deg(m)$. Prove that every element $\beta \in \mathbb{F}[\alpha]$ can be expressed **uniquely** as

$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{d-1}\alpha^{d-1} \quad \text{for some } b_0, b_1, \ldots, b_{d-1} \in \mathbb{F}.$$

[Hint: By definition of $\mathbb{F}[\alpha]$ we have $\beta = f(\alpha)$ for some polynomial $f(x) \in \mathbb{F}[x]$. Divide $f(x)$ by the minimal polynomial $m(x)$ to get $f(x) = m(x)q(x) + r(x)$.]

(d) Prove that $m(x)$ is irreducible over $\mathbb{F}$. [Hint: Suppose that $m(x) = f(x)g(x)$. Since $m(x)$ is in the kernel of φ_α we have $f(\alpha)g(\alpha) = m(\alpha) = 0$, and hence $f(\alpha) = 0$ or $g(\alpha) = 0$. If $f(\alpha) = 0$ then $f(x)$ is in the kernel of φ_α which implies that $m(x)|f(x)$.]

(e) Continuing from part (d), use the First Isomorphism Theorem and Problem 2(b) to show that $\mathbb{F}[\alpha]$ is a field.

4. Cube Roots of 2. Let $\alpha \in \mathbb{C}$ be any root of the polynomial $x^3 - 2 \in \mathbb{Q}[x]$.

(a) Prove that $x^3 - 2$ is irreducible over $\mathbb{Q}$, hence it is the minimal polynomial for α over $\mathbb{Q}$. [Hint: If $x^3 - 2$ is not irreducible over $\mathbb{Q}$ then it has a root $a/b \in \mathbb{Q}$ for some $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$. Use this to get a contradiction.]

(b) It follows from Problem 3 that the following set of numbers is a field:

$$\mathbb{Q}[\alpha] = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

Find the inverse of the number $1 + \alpha + \alpha^2$. [Hint: Let $(1 + \alpha + \alpha^2)(a + b\alpha + c\alpha^2) = 1 + 0\alpha + 0\alpha^2$. Expand the left side and equate coefficients. Use the fact that $\alpha^3 = 2$.]

---

[1] Recall: We say that $p \in R$ is prime when p is non-zero, non-unit, and $p = ab$ implies that a or b is a unit.

[2] The leading coefficient is 1.