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.]

(a): If $I = R$ then I contains all the units, and there is always at least one of these; namely, 1. Conversely, suppose that $u \in I$ for some unit $u \in R^\times$. Then since $u^{-1} \in R$ and $u \in I$ we have $1 = u^{-1}u \in I$. Finally, for any $a \in R$ we have $a \in R$ and $1 \in I$ hence $a = 1a \in I$.

(b): Let R be a field and consider an ideal $\{0\} \subsetneq I \subseteq R$. Since $I \neq \{0\}$ there exists a nonzero element $a \in I$, and since R is a field this element a is a unit. Hence $I = R$ by part (a).

(c): Let R be a ring with exactly two ideals: $\{0\}$ and R. To show that R is a field, consider any nonzero element $a \in R$ and the corresponding ideal aR. Since $a \neq 0$ we have $aR \neq \{0\}$. Since $\{0\}$ and R are the only ideals of R, this implies that $aR = R$. Finally, since $1 \in R = aR$, there exists some $b \in R$ such that $1 = ab$. Hence R is a field.

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 $x, y \in R$.]

(a): Consider an ideal $I \subseteq R$. If $I = \{0\}$ then $I = 0R$ is principal. Otherwise, consider a nonzero element $a \in I$ with minimum size $N(a)$. I claim that $I = aR$. On the one hand, since $a \in I$ we have for all $r \in R$ that $ar \in I$, and hence $aR \subseteq I$. On the other hand, consider any element $b \in I$ and divide by a to obtain $q, r \in R$ such that

$$\begin{cases} b = aq + r, \\ r = 0 \text{ or } N(r) < N(a). \end{cases}$$

Since $a, b \in I$ and $q \in R$ we have $r = b - aq \in I$. If $r \neq 0$ then r is a nonzero element of I that is smaller than a. Contradiction. Hence we must have $r = 0$ and hence $b = aq \in aR$. Since this holds for all $b \in I$ we have shown that $I \subseteq aR$ as desired.

(b): First suppose that $a \sim b$, so that $a = bu$ and $b = au^{-1}$ for some unit $u \in R^\times$. Then for all $r \in R$ we have $ar = b(ur) \in bR$, so that $aR \subseteq bR$. And for all $r \in R$ we have $br = a(u^{-1}r) \in aR$, so that $bR = aR$. It follows that $aR = bR$.

Conversely, suppose that $aR = bR$. If one of a or b is zero, then so is the other, hence $a \sim b$. So let us suppose that a, b are both nonzero. Since $a \in bR$ we have $a = bu$ for some $u \in R$

[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.

and since $b \in aR$ we have $b = av$ for some $v \in R$. Since R is an integral domain, we see that u and v are both units, hence $a \sim b$:

$$\begin{aligned} b &= av \\ b &= buv \\ b(1-uv) &= 0 \\ 1 - uv &= 0 && b \neq 0 \\ 1 &= uv. \end{aligned}$$

(c): Let $p \in R$ be prime and consider the ideal $pR \neq R$. I claim that the quotient ring R/pR is a field. To see this, consider any nonzero coset $a + pR \neq 0 + pR$, so that $a \notin pR$. In other words, we have $p \nmid a$. Since p is prime and $p \nmid a$ we must have $\gcd(a, p) = 1$, hence we can find some $b, c \in R$ satisfying $ab + pc = 1$. It follows $ab + pR = 1 + pR$, so that

$$(a + pR)(b + pR) = ab + pR = 1 + pR.$$

We have shown that any nonzero element of R/pR has a multiplicative inverse.

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.

(a): Let R be a ring satisfying $\mathbb{F} \subseteq R \subseteq \mathbb{F}[\alpha]$ and $\alpha \in R$. A general element of $\mathbb{F}[\alpha]$ looks like

$$\beta = a_0 + a_1\alpha + \cdots a_n\alpha^n,$$

for some $a_0, \ldots, a_n \in \mathbb{F}$. Then since $a_0, \ldots, a_n, \alpha \in R$ and since R is closed under addition and multiplication, we must have $\beta \in R$. Hence $R = \mathbb{F}[\alpha]$ as desired.

(b): If $\ker \varphi_\alpha = \{0\}$ then since $\mathbb{F}[x]$ is a PID we must have $\ker \varphi_\alpha = f(x)\mathbb{F}[x]$ for some $f(x) \in \mathbb{F}[x]$. Furthermore, if $f(x)\mathbb{F}[x] = g(x)\mathbb{F}[x]$ then from Problem 2(b) we must have $f(x) = \lambda g(x)$ for some nonzero constant $\lambda \in \mathbb{F}[x]$. It follows that there exists a unique monic polynomial $m(x) \in \mathbb{F}[x]$ such that $\ker \varphi_\alpha = m(x)\mathbb{F}[x]$. Indeed, we can take $m(x) = f(x)/\lambda$, where λ is the leading coefficient of $f(x)$. Then for any other monic polynomial $m'(x)$ satisfying

[2]The leading coefficient is 1.

$m(x)\mathbb{F}[x] = m'(x)\mathbb{F}[x]$ we must have $m(x) = \mu m'(x)$ for some constant μ. But since $m(x)$ and $m'(x)$ have the same leading coefficient, we must have $\mu = 1$ and hence $m(x) = m'(x)$.

(c): Let $m(x)$ be a generator of $\ker \varphi_\alpha$ and let $d = \deg(m)$. I claim that for any element $\beta \in \mathbb{F}[\alpha]$ there exist unique $b_0, \ldots, b_{d-1} \in \mathbb{F}$ such that

$$\beta = b_0 + b_1\alpha + \cdots + b_{d-1}\alpha^{d-1}.$$

Existence: By definition, any element of $\mathbb{F}[\alpha]$ looks like $\beta = f(\alpha)$ for some polynomial $f(x) \in \mathbb{F}[x]$. Divide $f(x)$ by the nonzero polynomial $m(x)$ to obtain

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

Since $r(x) = 0$ or $\deg(r) < \deg(m) = d$, we can write $r(x) = b_0 + b_1x + \cdots + b_{d-1}x^{d-1}$ for some elements $b_0, \ldots, b_{d-1} \in \mathbb{F}$ (possibly all zero). Then since $m(\alpha) = 0$ we have

$$\begin{aligned} \beta &= f(\alpha) \\ &= m(\alpha)q(\alpha) + r(\alpha) \\ &= r(\alpha) \\ &= b_0 + b_1\alpha + \cdots + b_{d-1}\alpha^{d-1}. \end{aligned}$$

Uniqueness: Suppose that we have

$$b_0 + b_1\alpha + \cdots + b_{d-1}\alpha^{d-1} = c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1}$$

for some $b_0, \ldots, b_{d-1}, c_0, \ldots, c_{d-1} \in \mathbb{F}$. We wish to show that $b_i = c_i$ for all i. To do this, we define the polynomials $r(x) = b_0 + b_1x + b_{d-1}x^{d-1}$ and $s(x) = c_0 + c_1x + \cdots + c_{d-1}x^{d-1}$. We will be done if we can show that $r(x) - s(x)$ is the zero polynomial, since then the coefficients of $r(x)$ and $s(x)$ will be equal.

By assumption we have $r(\alpha) = s(\alpha)$ and hence $r(\alpha) - s(\alpha) = 0$. In other words, we have $r(x) - s(x) \in \ker \varphi_\alpha$, which implies that $r(x) - s(x)$ is divisible by $m(x)$. If $r(x) - s(x) \neq 0$ then this gives a contradiction:

$$d = \deg(m) \leq \deg(r - s) \leq \max\{\deg(r), \deg(s)\} < d.$$

Hence $r(x) - s(x) = 0$ as desired.

(d): Let $m(x)$ be a generator of $\ker \varphi_\alpha$. To prove that $m(x)$ is irreducible over $\mathbb{F}$, suppose that we have $m(x) = f(x)g(x)$ for some (nonzero) $f(x), g(x) \in \mathbb{F}[x]$. Evaluating at $x = \alpha$ gives

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

which implies that $f(\alpha) = 0$ or $g(\alpha) = 0$. Without loss of generality, suppose that $f(\alpha) = 0$. Then since $f(x) \in \ker \varphi_\alpha$ we must have $m(x)|f(x)$. But since $m(x) = f(x)g(x)$ we also have $f(x)|m(x)$. It follows that $m(x) = \lambda f(x)$ for some constant $\lambda \in \mathbb{F}[x]$. Finally, since $f(x)g(x) = \lambda g(x)$, it follows that $g(x) = \lambda$ is constant. We have shown that

$$m(x) = f(x)g(x) \quad \Longrightarrow \quad f(x) \text{ or } g(x) \text{ is constant.}$$

In other words, $m(x)$ is irreducible over $\mathbb{F}$.

(e): If $\ker \varphi_\alpha = \{0\}$ then we have shown that $\ker \varphi_\alpha = m(x)\mathbb{F}[x]$ for a unique, monic polynomial $m(x) \in \mathbb{F}[x]$, which is irreducible. From the First Isomorphism Theorem we have

$$\mathbb{F}[\alpha] = \operatorname{im} \varphi_\alpha \cong \frac{\mathbb{F}[x]}{\ker \varphi_\alpha} = \frac{\mathbb{F}[x]}{m(x)\mathbb{F}[x]}.$$

Finally, since $m(x)$ is prime in $\mathbb{F}[x]$ we conclude from 2(c) that this quotient ring is a field.

Remark: This is a rather indirect way to prove that $\mathbb{F}[\alpha]$ is a field. In particular, it does not provide an algorithm to compute inverses in $\mathbb{F}[\alpha]$. The solution to this problem is to use 3(c) to express $\mathbb{F}[\alpha]$ as a vector space over $\mathbb{F}$ with basis $1, \alpha, \ldots, \alpha^{d-1}$ and then use linear algebra.

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 $\alpha^3 = 2$.]

(a): Let $\alpha \in \mathbb{C}$ satisfy $\alpha^3 - 2 = 0$, let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and let $m(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$, so that $m(x)|f(x)$. I claim that in fact $m(x) = f(x)$.To show this, it is enough to prove that $f(x)$ is irreducible over $\mathbb{Q}$, since then $m(x)|f(x)$ implies $m(x) = \lambda f(x)$ and since $f(x), m(x)$ are both monic we must have $\lambda = 1$.

So suppose for contradiction that $f(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathbb{Q}[x]$, both non-constant. By comparing degrees we must have $\deg(f) = 1$ or $\deg(g) = 1$. Without loss of generality, suppose that $\deg(f) = 1$, so that $f(x) = \alpha x + \beta$ with $\alpha, \beta \in \mathbb{Q}$ and $\alpha \neq 0$. Write $-\beta/\alpha = a/b$ for some $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$. Then we have

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

which implies that

$$\begin{aligned} (a/b)^3 - 2 &= 0 \\ a^3 - 2b^3 &= 0 \\ a^3 &= 2b^3. \end{aligned}$$

Since $a|2b^3$ and $\gcd(a, b) = 1$ we must have $a|2$ and since $b|a^3$ we must have $b|1$. It follows that a/b is ± 1 or ± 2.[3] But none of these four numbers is a root of $x^3 - 2$. Contradiction.

(b): If $\alpha^3 - 2 = 0$ then we have shown that $x^3 - 2$ is the minimal polynomial of α over $\mathbb{Q}$. Since $\deg(x^3 - 2) = 3$ this implies that the field $\mathbb{Q}[\alpha] \subseteq \mathbb{C}$ can be expressed as a vector space over $\mathbb{Q}$ with basis $1, \alpha, \alpha^2$:

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

This representation allows us to do computations in $\mathbb{Q}[\alpha]$ via linear algebra. For example, we compute the inverse of the nonzero element $1 + \alpha + \alpha^2 \in \mathbb{Q}[\alpha]$. The inverse must have the form $a + b\alpha + c\alpha^2$ for some $a, b, c \in \mathbb{Q}$ where

$$(1 + \alpha + \alpha^2)(a + b\alpha + c\alpha^2) = 1 + 0\alpha + 0\alpha^2.$$

[3] We have just performed the "rational root test", to find a finite list of potential roots of $x^3 - 2$ in $\mathbb{Q}$.

Expanding the left hand side and using the fact that $\alpha^3 - 2 = 0$ gives

$$\begin{aligned}
(1+\alpha+\alpha^2)(a+b\alpha+c\alpha^2) &= a + b\alpha + c\alpha^2 \\
&\quad a\alpha + b\alpha^2 + c\alpha^3 \\
&\quad a\alpha^2 + b\alpha^3 + c\alpha^4 \\
&= a + b\alpha + c\alpha^2 \\
&\quad a\alpha + b\alpha^2 + 2c \\
&\quad a\alpha^2 + 2b + 2c\alpha \\
&= (a+2b+2c) + (a+b+2c)\alpha + (a+b+c)\alpha^2.
\end{aligned}$$

Then comparing coefficients[4] gives a system of three linear equations in the unknowns a, b, c:

$$\begin{cases}
a + 2b + 2c = 1, \\
a + b + 2c = 0, \\
a + b + c = 0.
\end{cases}$$

After a bit of work we find that $(a, b, c) = (-1, 1, 0)$, so that

$$(1+\alpha+\alpha^2)(-1+\alpha) = 1.$$

Remark: With a bit more work we can find a formula for the inverse of a general element $r+s\alpha+t\alpha^2$. By expanding $(r+s\alpha+t\alpha^2)(a+b\alpha+c\alpha^2) = 1+0\alpha+0\alpha^2$ we obtain the following system of linear equations in a, b, c:

$$\begin{cases}
ra + 2tb + 2sc = 1, \\
sa + rb + 2tc = 0, \\
ta + sb + rc = 0.
\end{cases}$$

Then my computer gives the following solution:

$$(a, b, c) = \frac{1}{r^3 + 2s^3 + 4t^3 - 6rst}\left(r^2 - 2st, rs - 2t^2, rt - s^2\right).$$

That is, for any $r, s, t \in \mathbb{Q}$, not all zero, we have

$$\frac{1}{r+s\alpha+t\alpha^2} = \frac{1}{r^3 + 2s^3 + 4t^3 - 6rst}\left((r^2 - 2st) + (rs - 2t^2)\alpha + (rt - s^2)\alpha^2\right).$$

As an interesting consequence, if $r, s, t \in \mathbb{Q}$ are not all zero then we must have

$$r^3 + 2s^3 + 4t^3 - 6rst \neq 0.$$

I have no idea how I would prove this by other methods.

[4] We can do this because of uniqueness.