Math 562 **Spring 2014**
Exam 3 — Thurs Apr 24 **Drew Armstrong**

There are 3 problems with 12 parts. Each part is worth 2 points, for a total of 24 points.

1. Let K be a field.

(a) Accurately state the Division Theorem for $K[x]$. [Hint: "Given two polynomials $f(x), g(x) \in K[x]$ with $g(x) \neq 0$ there exist $q(x), r(x) \in K[x]$ such that…"]

Proof. Given two polynomials $f(x), g(x) \in K[x]$ with $g(x) \neq 0$ there exist $q(x), r(x) \in K[x]$ such that
- $f(x) = q(x)g(x) + r(x)$,
- $r(x) = 0$ or $\deg(r) < \deg(g)$.

□

(b) Consider $\alpha \in K$ and $f(x) \in K[x]$. If $f(\alpha) = 0$, prove that $(x - \alpha)$ divides $f(x)$ in $K[x]$. [Hint: Use part (a).]

Proof. Assume that $f(\alpha) = 0$. Since $0 \neq x - \alpha \in K[x]$, part (a) says that there exist $q(x), r(x) \in K[x]$ such that
- $f(x) = q(x)(x - \alpha) + r(x)$,
- $r(x) = 0$ or $\deg(r) < \deg(x - \alpha) = 1$.

The second condition says that $r(x) = r \in K$ is a constant. Then evaluating the first condition at α gives

$$0 = f(\alpha) = q(\alpha)(\alpha - \alpha) + r = q(\alpha) \cdot 0 + r = 0 + r = r.$$

We conclude that $f(x) = q(x)(x - \alpha)$. □

(c) Let $f(x) \in K[x]$ have degree 3. If $f(x)$ is **not** irreducible in $K[x]$, prove that $f(x)$ has a root in K.

Proof. Suppose that we have $f(x) = g(x)h(x)$ where $\deg(g) \geq 1$ and $\deg(h) \geq 1$ (i.e. g and h are not units). Then since

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

we conclude that $\deg(g) = 1$ or $\deg(h) = 1$. Without loss, assume that $\deg(g) = 1$ so that $g(x) = ax + b$ for some $a, b \in K$ with $a \neq 0$. Then we have

$$f(-b/a^{-1}) = g(-b/a^{-1})h(-b/a^{-1}) = 0 \cdot h(-b/a^{-1}) = 0,$$

hence $f(x)$ has the root $-b/a^{-1} \in K$. □

(d) Let $\mathbb{F}_3 = \{0, 1, 2\}$ be the field with three elements. Prove that the polynomial $x^3 + 2x + 1$ is irreducible in $\mathbb{F}_3[x]$. [Hint: Use part (c).]

Proof. By part (c) it is enough to check that $x^3 + 2x + 1 \in \mathbb{F}_3[x]$ has no root in $\mathbb{F}_3$. Since $\mathbb{F}_3$ only has 3 elements we can check them all:

$$0^3 + 2 \cdot 0 + 1 = 1 \neq 0$$
$$1^3 + 2 \cdot 1 + 1 = 4 = 1 \neq 0$$
$$2^3 + 2 \cdot 2 + 1 = 13 = 1 \neq 0.$$

□

2. Let $L \supseteq K$ be a field extension. Given $\alpha \in L$ we define the evaluation homomorphism $\mathsf{ev}_\alpha : K[x] \to L$ by sending $\sum_k a_k x^k \mapsto \sum_k a_k \alpha^k$. Assume that ev_α is not injective (i.e. that α is "algebraic" over K).

(a) State the definition of the minimal polynomial $m_\alpha(x) \in K[x]$ and say why it exists.

Proof. We know that $\ker(\mathsf{ev}_\alpha)$ is a nonzero ideal of $K[x]$. Since $K[x]$ is a PID this implies that $\ker(\mathsf{ev}_\alpha) = (m_\alpha(x))$ for some nonzero polynomial $m_\alpha(x) \in K[x]$. If we assume that the leading coefficient of $m_\alpha(x)$ is 1 then this polynomial is unique and we call it the minimal polynomial of α over K. □

(b) Prove that $m_\alpha(x)$ is irreducible over K. [Hint: Suppose for contradiction that there is a nontrivial factorization $m_\alpha(x) = f(x)g(x)$.]

Proof. Assume for contradiction that we have $m_\alpha(x) = f(x)g(x)$ for some $f(x), g(x) \in K[x]$ with $\deg(f) < \deg(m_\alpha)$ and $\deg(g) < \deg(m_\alpha)$. Evaluating at α gives

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

and since L is a domain this implies $f(\alpha) = 0$ or $g(\alpha) = 0$. Without loss, suppose that $f(\alpha) = 0$. This implies that $f(x) \in \ker(\mathsf{ev}_\alpha) = (m_\alpha(x))$ and hence $m_\alpha(x)$ divides $f(x)$. Since $f(x) \neq 0$ this implies $\deg(m_\alpha) \leq \deg(f)$, which contradicts the fact that $\deg(f) < \deg(m_\alpha)$. □

(c) Prove that the image $K[\alpha] := \mathrm{im}(\mathsf{ev}_\alpha)$ is a field. [Hint: Use part (b).]

Proof. Since $m_\alpha(x)$ is irreducible, the ideal $(m_\alpha) < K[x]$ is maximal among principal ideals. Since $K[x]$ is a PID this implies that (m_α) is maximal among **all** ideals, which by the Correspondence Theorem implies that $K[x]/(m_\alpha)$ is a field. Finally, we use the First Isomorphism Theorem to conclude that

$$K[\alpha] = \mathrm{im}(\mathsf{ev}_\alpha) \approx \frac{K[x]}{\ker(\mathsf{ev}_\alpha)} = \frac{K[x]}{(m_\alpha)}$$

is a field. □

(d) If $S \subseteq L$ is any subring of L containing the set $K \cup \{\alpha\}$, prove that $K[\alpha] \subseteq S$.

Proof. A general element of $K[\alpha]$ looks like $f(\alpha) = \sum_k a_k \alpha^k$ where $f(x) = \sum_k a_k x^k \in K[x]$. Since $\alpha \in S$ and $a_k \in S$ for all $a_k \in S$, and since S is closed under addition and multiplication, we conclude that

$$f(\alpha) = \sum_k a_k \alpha^k \in S.$$

□

3. Consider the ring $\mathbb{F}_3[x]$ where $\mathbb{F}_3 = \{0, 1, 2\}$ is the field with three elements. Kronecker's Theorem says that there exists a field extension $L \supseteq \mathbb{F}_3$ and an element $\alpha \in L$ such that $\alpha^3 + 2\alpha + 1 = 0$.

(a) Prove that the minimal polynomial of α over $\mathbb{F}_3$ is $m_\alpha(x) = x^3 + 2x + 1$. [Hint: Use Problem 1(d).]

Proof. Let $f(x) = x^3 + 2x + 1 \in \mathbb{F}_3[x]$ and let $m_\alpha(x) \in \mathbb{F}_3[x]$ be the minimal polynomial of $\alpha \in L$ over $\mathbb{F}_3[x]$. Since $f \in \ker(\mathsf{ev}_\alpha) = (m_\alpha)$ we conclude that m_α divides f. Since $f(x)$ is irreducible (by Problem 1(d)) this implies that $m_\alpha(x)$ is a nonzero constant or is associate to $f(x)$. But since $m_\alpha(\alpha) = 0$ we know that $m_\alpha(x)$ is not a nonzero constant. Hence $m_\alpha(x)$ and $f(x)$ are associate. Since we assume that $m_\alpha(x)$ has leading coefficient 1 this implies that $m_\alpha(x) = f(x)$. $\square$

(b) By Problem 2(c) we know that $\mathbb{F}_3[\alpha]$ is a field. Prove that every element of this field has the form $a + b\alpha + c\alpha^2$ for some $a, b, c \in \mathbb{F}_3$. [Hint: A general element of $\mathbb{F}_3[\alpha]$ looks like $f(\alpha)$ for some $f(x) \in \mathbb{F}_3[x]$.]

Proof. A general element of $\mathbb{F}_3[\alpha]$ looks like $f(\alpha)$ for some $f(x) \in \mathbb{F}_3[x]$. We can divide $f(x)$ by the minimal polynomial $m_\alpha(x)$ to obtain

- $f(x) = q(x)m_\alpha(x) + r(x)$,
- $r(x) = 0$ or $\deg(r) < \deg(m_\alpha) = 3$.

Evaluating at α gives

$$f(\alpha) = q(\alpha)m_\alpha(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha).$$

Since $\deg(r) < 3$ we can write $r(x) = a + bx + cx^2$ for some $a, b, c \in \mathbb{F}_3$. Then we have $f(\alpha) = r(\alpha) = a + b\alpha + c\alpha^2$. $\square$

(c) Compute the size of the field $\mathbb{F}_3[\alpha]$. [Hint: You may assume without proof that the set $1, \alpha, \alpha^2$ is linearly independent over $\mathbb{F}_3$.]

Proof. We know from part (b) that every element of $\mathbb{F}_3[\alpha]$ can be written as $a + b\alpha + c\alpha^2$ for some $a, b, c \in \mathbb{F}_3$, and we assume without proof that this representation is unique. Thus we have a bijection between elements of $\mathbb{F}_3[\alpha]$ and vectors $(a, b, c) \in (\mathbb{F}_3)^3$. It follows that

$$|\mathbb{F}_3[\alpha]| = |\mathbb{F}_3|^3 = 3^3 = 27.$$

$\square$

(d) Compute the product of $1 + \alpha + \alpha^2$ and $1 + 2\alpha$ in the field $\mathbb{F}_3[\alpha]$.

Proof. First we note that

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

Then we use the fact that $\alpha^3 = -2\alpha - 1 = \alpha + 2$ to obtain

$$\begin{aligned}1 + 2\alpha^3 &= 1 + 2(\alpha + 2) \\ &= 1 + 2\alpha + 4 \\ &= 5 + 2\alpha \\ &= 2 + 2\alpha.\end{aligned}$$

We conclude that $(1 + \alpha + \alpha^2)(1 + 2\alpha) = 2 + 2\alpha$. The other $\binom{27}{2} - 1 = 350$ products are left to the reader. $\square$