MTH 562/662 **Spring 2019**
Exam 2 — Fri Apr 5 **Drew Armstrong**

Problem 1. Let R be an integral domain and assume that $R[x]$ is a PID.

(a) Prove that $x \in R[x]$ is irreducible.

Suppose that $x = f(x)g(x)$ for some polynomials $f(x), g(x) \in R[x]$. Since R is a domain this implies that $\deg(f) + \deg(g) = \deg(x) = 1$, hence at least one of $f(x)$ or $g(x)$ has degree zero, i.e., is a unit.

(b) Use the fact that $R[x]$ is a PID to prove that $\langle x \rangle \subseteq R[x]$ is a maximal ideal.

Since $x \in R[x]$ is irreducible we know that $\langle x \rangle$ is maximal among principal ideals. Since $R[x]$ is a PID this implies that $\langle x \rangle$ is maximal among all ideals.

(c) Prove that $R \cong R[x]/\langle x \rangle$ and hence R is a field.

Consider the map $\varphi := R[x] \to R$ defined by $f(x) \mapsto f(0)$. This is a surjective ring homomorphism with kernel $\langle x \rangle$. Hence by the First Isomorphism Theorem we have

$$R[x]/\langle x \rangle = R[x]/\ker\varphi \cong \operatorname{im}\varphi = R.$$

Since $\langle x \rangle$ is a maximal ideal this implies that R is a field.

Problem 2. Let $\alpha \in \mathbb{E} \supseteq \mathbb{F}$ be an element of a field extension and consider the evaluation homomorphism $\mathrm{id}_\alpha : \mathbb{F}[x] \to \mathbb{E}$ defined by $f(x) \mapsto f(\alpha)$. You may assume that $\ker(\mathrm{id}_\alpha) = \langle m(x) \rangle \neq \{0\}$ is a **maximal** ideal with $d := \deg(m)$.

(a) Let $\mathbb{F}[\alpha] = \mathrm{im}(\mathrm{id}_\alpha) \subseteq \mathbb{E}$ and let $\mathbb{F}(\alpha) \subseteq \mathbb{E}$ be the smallest subfield containing $\mathbb{F} \cup \{\alpha\}$. Prove that $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$.

Since $\langle m(x) \rangle$ is maximal, the First Isomorphism Theorem tells us that $\mathbb{F}[\alpha]$ is a field:

$$R[x]/\langle m(x) \rangle = R[x]/\ker(\mathrm{id}_\alpha) \cong \mathrm{im}(\alpha_\alpha) = \mathbb{F}[\alpha].$$

Since $\mathbb{F}[\alpha]$ contains the set $\mathbb{F} \cup \{\alpha\}$ this implies that $\mathbb{F}(\alpha) \subseteq \mathbb{F}[\alpha]$. Conversely, let $f(\alpha)$ be any element of $\mathbb{F}[\alpha]$. Since $\mathbb{F}(\alpha)$ contains $\mathbb{F} \cup \{\alpha\}$ and is closed under addition and multiplication we conclude that $f(\alpha) \in \mathbb{F}(\alpha)$, hence $\mathbb{F}[\alpha] \subseteq \mathbb{F}(\alpha)$.

(b) Use part (a) to prove that every element of $\mathbb{F}(\alpha)$ can be written in the form $a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$ for some $a_0, \ldots, a_{d-1} \in \mathbb{F}$. [Hint: Division with remainder.]

Every element of $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$ has the form $f(\alpha)$ for some polynomial $f(x) \in \mathbb{F}[x]$. Divide by $f(x)$ by $m(x)$ to obtain $q(x), r(x) \in \mathbb{F}[x]$ such that

$$f(x) = q(x)m(x) + r(x) \quad \text{and} \quad \deg(r) < \deg(m) = d.$$

Then we have

$$\begin{aligned} f(\alpha) &= q(\alpha)m(\alpha) + r(\alpha) \\ &= q(\alpha)0 + r(\alpha) \\ &= r(\alpha) \end{aligned}$$

$$= a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$$

for some $a_0, \ldots, a_{d-1} \in \mathbb{F}$.

(c) Prove that the expression in part (b) is unique. [Hint: Suppose $r(\alpha) = 0$ for some polynomial $r(x) \in \mathbb{F}[x]$ of degree $< d$.]

Suppose that

$$a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} = b_0 + a_1\alpha + \cdots + b_{d-1}\alpha^{d-1}$$

for some $a_i, b_i \in \mathbb{F}$. This implies that $r(\alpha) = 0$ where $r(x) = \sum_i (a_i - b_i)x^i$ has degree $< d$. Then by definition of $m(x)$ we have $m(x)|r(x)$, which is a contradiction unless $r(x) = 0$ and hence $a_i = b_i$ for all i.

Problem 3. Let $\mathbb{E}$ be a field of size p^k.

(a) Let $\mathbb{F} \subseteq \mathbb{E}$ be the image of the unique ring homomorphism $\mathbb{Z} \to \mathbb{E}$. Prove that $\mathbb{F} \cong \mathbb{F}_p$.

You can feel free to quote the theorem on prime subfields, but I'm going to prove it. Let $\varphi : \mathbb{Z} \to \mathbb{E}$ be the unique ring homomorphism from $\mathbb{Z}$. Then since $\ker \varphi = n\mathbb{Z}$ is principal we have

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{F} \subseteq \mathbb{E}.$$

Since $\mathbb{E}$ is finite we have $n \neq 0$ and since $\mathbb{F}$ (being a subring of a field) is a domain we conclude that $n\mathbb{Z}$ is a prime ideal, hence $n = p$ is prime.

(b) Use Lagrange's Theorem to show that $\alpha^{p^k-1} = 1$ for all non-zero $\alpha \in \mathbb{E}$.

The group of non-zero elements $(\mathbb{E}^\times, \times, 1)$ has size $p^k - 1$. By Lagrange's Theorem it follows that $\alpha^{p^k-1} = 1$ for all $\alpha \in \mathbb{E}^\times$.

(c) Prove that $\mathbb{E}$ is a splitting field for $x^{p^k} - x \in \mathbb{F}_p[x]$.

Let $f(x) = x^{p^k} - x \in \mathbb{F}_p[x]$. Clearly we have $f(0) = 0$ and from (b) we know that $f(\alpha) = 0$ for all $\alpha \in \mathbb{E}^\times$. Since $f(x)$ has degree p^k it follows that $f(x)$ splits over $\mathbb{E}$:

$$f(x) = \prod_{\alpha \in \mathbb{E}} (x - \alpha) \in \mathbb{E}[x].$$

Furthermore, since the polynomial $f(x)$ has p^k distinct roots in $\mathbb{E}$, it cannot split over any subfield of $\mathbb{E}$.

Problem 4. Let $\alpha = \sqrt[6]{2} \in \mathbb{R}$ and $\omega = e^{2\pi i/6} = (1 + i\sqrt{3})/2$.

(a) Prove that $\mathbb{Q}(\alpha, \omega)$ is the splitting field of $x^6 - 2$ over $\mathbb{Q}$.

The six roots of $x^6 - 2$ are $\{\alpha, \omega\alpha, \omega^2\alpha, \omega^3\alpha, \omega^4\alpha, \omega^5\alpha\}$, hence the splitting field is

$$\mathbb{E} := \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha, \omega^3\alpha, \omega^4\alpha, \omega^5\alpha).$$

Since all six roots are in $\mathbb{Q}(\alpha, \omega)$ we have $\mathbb{E} \subseteq \mathbb{Q}(\alpha, \omega)$. On the other hand, since $\alpha \in \mathbb{E}$ and $\omega = (\omega\alpha)/\alpha \in \mathbb{E}$ we have $\mathbb{Q}(\alpha, \omega) \subseteq \mathbb{E}$.

(b) Prove that $x^2 - x + 1$ is the minimal polynomial of ω over $\mathbb{Q}(\alpha)$. [Hint: $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$.]

You may recall that $\Phi_6(x) = x^2 - x + 1$. Otherwise, one can check directly that

$$x^2 - x + 1 = (x - \omega)(x - \omega^5) = (x - \omega)(x - \omega^{-1}).$$

Since this polynomial has degree 2 and no real roots, it is irreducible over $\mathbb{Q}(\alpha)$.

(c) **Assuming** that $x^6 - 2 \in \mathbb{Q}[x]$ is irreducible, prove that $[\mathbb{Q}(\alpha, \omega)/\mathbb{Q}] = 12$.

Consider the chain of field extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha)(\omega) = \mathbb{Q}(\alpha, \omega).$$

If $x^2 - 6$ is irreducible over $\mathbb{Q}$ then since $\alpha^6 - 2 = 0$ we have $[\mathbb{Q}(\alpha)/\mathbb{Q}] = 6$, and from part (b) we have $[\mathbb{Q}(\alpha, \omega)/\mathbb{Q}(\alpha)] = 2$. It follows from Dedekind's Tower Law that

$$[\mathbb{Q}(\alpha, \omega)/\mathbb{Q}] = [\mathbb{Q}(\alpha, \omega)/\mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha)/\mathbb{Q}] = 2 \cdot 6 = 12.$$

Problem 5 (optional). What is Sanjoy's Kundu's favorite Pokémon?

Sanjoy named his favorite Pokémon from each generation. His first generation favorite is Pikachu. Gregory said Charmander. David said "Pokémon."