Math 562/662 **Spring 2022**
Homework 6 **Drew Armstrong**

---

1. Irreducible Polynomials of Small Degree. Let $\mathbb{F}$ be a field and consider a polynomial $f(x) \in \mathbb{F}[x]$ of degree 2 or 3. Prove that $f(x)$ is irreducible over $\mathbb{F}$ if and only if $f(x)$ has no root in $\mathbb{F}$. [Hint: Equivalently, prove that $f(x)$ if reducible if and only if has a root.]

Proof. We will show that $f(x)$ is reducible if and only if has a root in $\mathbb{F}$. First suppose that $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}$. Then from Descartes we have $f(x) = (x - \alpha)g(x)$ where $g(x) \in \mathbb{F}[x]$ and $\deg(g) = \deg(f) - 1 \geq 1$, and it follows that $f(x)$ is reducible.

Conversely, suppose that $f(x) = g(x)h(x)$ for some non-constant $g(x), h(x) \in \mathbb{F}[x]$. Since $\deg(g), \deg(h) \geq 1$ and $\deg(g) + \deg(h) = \deg(f) = 2$ or 3 this implies that one of $g(x), h(x)$ has degree 1. Say $\deg(g) = 1$. This means that $g(x) = ax + b$ for some $a, b \in \mathbb{F}$ with $a \neq b$. But then $g(-b/a) = 0$ implies

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

and hence $f(x)$ has a root $-b/a \in \mathbb{F}$.

2. Rational Roots. Consider a polynomial of degree $n \geq 1$ with integer coefficients:

$$f(x) = c_0 + c_1x + \cdots + c_nx^n \in \mathbb{Z}[x].$$

If $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, prove that we must have $a|c_0$ and $b|c_n$. Use this result and Problem 1 to prove that the polynomial $4x^3 + 29x - 3$ is irreducible over $\mathbb{Q}$.

Proof. Suppose that $f(\alpha) = 0$ for some $\alpha \in \mathbb{Q}$ and write $\alpha = a/b$ with $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$. Substitute and multiply both sides by b^n to obtain

$$\begin{aligned} f(a/b) &= 0 \\ c_0 + c_1(a/b) + \cdots + c_n(a/b)^n &= 0 \\ c_0b^n + c_1ab^{n-1} + \cdots + c_na^n &= 0. \end{aligned}$$

The equation $-c_na^n = b(c_0b^{n-1} + c_1ab^{n-2} + \cdots + c_{n-1}a^{n-1})$ implies that $b|c_na^n$, which implies that $b|c_n$ because $\gcd(a, b) = 1$. And the equation $-c_0b^n = a(c_1b^{n-1} + c_2ab^{n-2} + \cdots + c_na^{n-1})$ implies that $a|c_0b^n$, which implies that $a|c_0$ because $\gcd(a, b) = 1$. $\square$

For example, if $f(x) = 4x^3 + 29x - 3$ has a rational root $a/b \in \mathbb{Q}$ written in lowest terms, then we must have $a|3$ and $b|4$, so that $a/b \in \{\pm 1, \pm 1/2, \pm 1/4, \pm 3, \pm 3/2, \pm 3/4\}$. But none of these potential roots is actually a root:

$$\begin{aligned} f(1) &= 30, \\ f(-1) &= -36, \\ f(1/2) &= 12, \\ f(-1/2) &= -18, \\ f(1/4) &= 69/16, \\ f(-1/4) &= -165/16, \\ f(3) &= 34, \\ f(-3) &= -32, \end{aligned}$$

$$\begin{aligned} f(3/2) &= 54, \\ f(-3/2) &= -60, \\ f(3/4) &= 327/16, \\ f(-3/4) &= -423/16. \end{aligned}$$

Hence $f(x)$ has no rational root. Since $\deg(f) = 3$ it follows from Problem 1 that $f(x)$ is irreducible over $\mathbb{Q}$.

3. Repeated Roots. For any field $\mathbb{F}$ we define the function $D : \mathbb{F}[x] \to \mathbb{F}[x]$ by[1]

$$D\left(\sum a_k x^k\right) = \sum k \cdot a_k x^{k-1}.$$

This *formal derivative* satisfies all the usual properties, such as the product rule. Now consider a polynomial $f(x) \in \mathbb{F}[x]$ and an element of a field extension $\alpha \in \mathbb{E} \supseteq \mathbb{F}$.

(a) If $f(x) = (x - \alpha)^2 g(x)$ for some $g(x) \in \mathbb{E}[x]$, prove that $f(\alpha) = 0$ and $Df(\alpha) = 0$.
(b) Conversely, suppose that $f(\alpha) = 0$ and $Df(\alpha) = 0$. In this case, prove that there exists a polynomial $g(x) \in \mathbb{E}[x]$ such that $f(x) = (x - \alpha)^2 g(x)$. [Hint: Use Descartes' Factor Theorem twice.]

(a): Consider an element of a field extension, $\alpha \in \mathbb{E} \supseteq \mathbb{F}$, and suppose that $f(x) = (x-\alpha)^2 g(x)$ for some polynomials $f(x), g(x) \in \mathbb{F}[x]$. First we observe that

$$f(\alpha) = (\alpha - \alpha)^2 g(\alpha) = 0.$$

Next we take the derivative of $f(x)$:

$$Df(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 Dg(x).$$

It follows that

$$Df(\alpha) = 2(\alpha - \alpha)g(\alpha) + (\alpha - \alpha)^2 Dg(\alpha) = 0.$$

(b): Consider an element of a field extension, $\alpha \in \mathbb{E} \supseteq \mathbb{F}$, and consider a polynomial $f(x) \in \mathbb{F}[x]$ such that $f(\alpha) = 0$ and $Df(\alpha) = 0$. Since $f(\alpha) = 0$ Descartes' Factor Theorem tells us that

$$f(x) = (x - \alpha)g(x) \text{ for some } g(x) \in \mathbb{F}[x].$$

Now take the derivative to obtain

$$Df(x) = g(x) + (x - \alpha)Dg(x).$$

Then since $Df(\alpha) = 0$ we have

$$0 = Df(\alpha) = g(\alpha) + (\alpha - \alpha)Dg(\alpha) = g(\alpha).$$

Finally, since $g(\alpha) = 0$, Descartes tells us that $g(x) = (x - \alpha)h(x)$ for some $h(x) \in \mathbb{F}[x]$, hence

$$f(x) = (x - \alpha)g(x) = (x - \alpha)(x - \alpha)h(x) = (x - \alpha)^2 h(x).$$

[1] Given $k \in \mathbb{Z}$ and $a_k \in \mathbb{F}$, the element $k \cdot a_k \in \mathbb{F}$ is defined repeated addition or subtraction. See Problem 4.

4. Characteristic of a Field. For any field $\mathbb{F}$, we have seen that there exists a unique group homomorphism $\varphi : (\mathbb{Z}, +, 0) \to (\mathbb{F}, +, 0)$ sending 1 to 1. Namely,[2]

$$\varphi(k) = k \cdot 1 := \begin{cases} \overbrace{1 + 1 + \cdots + 1}^{k \text{ times}} & \text{if } k \geq 1, \\ 0 & \text{if } k = 0, \\ \underbrace{-1 - 1 - \cdots - 1}_{-k \text{ times}} & \text{if } k \leq -1. \end{cases}$$

One can check that this function $\varphi : \mathbb{Z} \to \mathbb{F}$ is also a ring homomorphism. If $\ker \varphi = n\mathbb{Z}$ then we say that $\mathrm{char}(\mathbb{F}) := n$ is the *characteristic of the field* $\mathbb{F}$.

(a) If $\mathbb{F}$ is finite, show that $\mathrm{char}(\mathbb{F}) \neq 0$. [Hint: The First Isomorphism Theorem says that $\mathbb{Z}/\ker\varphi \cong \operatorname{im}\varphi$, where $\operatorname{im}\varphi$ is a subring of $\mathbb{F}$. But $\mathbb{Z}/0\mathbb{Z}$ is infinite.]
(b) If $n \geq 1$ is not prime, show that $\mathbb{Z}/n\mathbb{Z}$ is not a domain.
(c) If $\mathbb{F}$ is finite, combine (a) and (b) to show that the characteristic $\mathrm{char}(\mathbb{F})$ is prime. [Hint: A subring of a field is necessarily a domain.]

(a): The hint says it all.

(b): Suppose that $n \geq 1$ is not prime; say $n = ab$ where $1 < a, b < n$. Then in $\mathbb{Z}/n\mathbb{Z}$ we have

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z} = n + n\mathbb{Z} = 0 + n\mathbb{Z}.$$

But since $1 < a, b < n$ we have $a + n\mathbb{Z} \neq 0 + n\mathbb{Z}$ and $b + n\mathbb{Z} \neq 0 + n\mathbb{Z}$.

(c): Let $\mathbb{F}$ be a finite field and consider the unique ring homomorphism $\varphi : \mathbb{Z} \to \mathbb{F}$. The kernel of φ, being an ideal of $\mathbb{Z}$, must be $n\mathbb{Z}$ for some $n \geq 0$. Then from the First Isomorphism Theorem we have

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker\varphi \cong \operatorname{im}\varphi \subseteq \mathbb{F}.$$

Since $\mathbb{F}$ is finite we see that $\operatorname{im}\varphi$ and hence $\mathbb{Z}/n\mathbb{Z}$ is finite, which implies that $n \geq 1$. Then since $\mathbb{F}$ is a field, the subring $\operatorname{im}\varphi$ must be a domain. Indeed, suppose that we have $ab = 0$ for some $a, b \in \operatorname{im}\varphi$. If $a = 0$ then we are done, so suppose that $a \neq 0$. Then since the inverse $a^{-1} \in \mathbb{F}$ exists we have

$$\begin{aligned} ab &= 0 \\ aa^{-1} &= a^{-1}0 \\ b &= 0. \end{aligned}$$

Finally, since $\mathbb{Z}/n\mathbb{Z} \cong \operatorname{im}\varphi$ is a domain, it follows from part (b) that n is prime.

Remark: It follows that any finite field $\mathbb{E}$ contains a subfield isomorphic to $\mathbb{F}_p$ for some prime p. Then since $\mathbb{E}$ is a vector space over $\mathbb{F}_p$ it follows from linear algebra[3] that there exists a (non-unique) finite basis $\alpha_1, \ldots, \alpha_k \in \mathbb{E}$ so that every $\beta \in \mathbb{E}$ has a unique expression

$$\beta = b_1\alpha_1 + b_2\alpha_2 + \cdots + b_k\alpha^k,$$

[2]Previously we used the multiplicative notation $\varphi(a) = a^k$ but the concept is the same.

[3]Start with the whole field $S = \mathbb{E}$. If any element of S is expressible as an $\mathbb{F}_p$-linear combination of the other elements of S, throw it away. Continue until no element of S is expressible as an $\mathbb{F}_p$-linear combination of the others. The result will be the desired basis.

with $b_1, \ldots, b_k \in \mathbb{F}_p$. In other words, we have a bijection between $\mathbb{E}$ and the set of k-tuples of elements from $\mathbb{F}_p$. It follows that

$$\#\mathbb{E} = (\#\mathbb{F}_p)^k = p^k.$$

In class we proved that a field of size p^k exists for every prime power p^k and that any two finite fields of size p^k are isomorphic. But these existence and uniqueness results are not on the exam.