David Owen Horace Cutler

Math 146: Homework 4

March 1, 2024

Exercise 1. Let F be a field and let $f \in F[x]$ be a monic polynomial. Prove that f is irreducible if and only if f cannot be factored as a product of two *monic* polynomials of smaller degree.

Proof. Remark the forward direction is trivially true, as irreducibility specifically means that f cannot be factored into **any** two polynomials of smaller degree.

We will prove the reverse direction then, that is that if f cannot be factored as a product of two monic polynomials of smaller degree, then f is irreducible.

For this, we will consider the contrapositive that is that f being reducible implies that f can be factored as a product of two monic polynomials of smaller degree.

We first remark that as f is reducible, it admits a factorization as follows:

$$\begin{gathered} f = gh \\ \deg(g),\ \deg(h) < \deg(f) \end{gathered} \tag{1}$$

In particular, we may write $g = \sum_{i=0}^{N} a_i x^i$ and $h = \sum_{j=0}^{M} b_j x^j$ where $N, M < \deg(f)$ and $a_N, b_M \neq 0$. We recall then the product formula for gh, that is:

$$gh = \sum_{l=0}^{N+M} \Big(\sum_{\substack{i+j=l \\ i,j \in \mathbb{N}}} a_i b_j \Big) x^l \tag{2}$$

Taking $l = N + M$ then demonstrates that the $N + M$ degree coefficient of $gh = f$ is $a_N b_M$. As f is monic then, it must be than $a_N b_M = b_M a_N = 1$, i.e. a_N and b_M are multiplicative inverses of each other.

Using that $F[x]$ is a commutative ring then, we get the following:

$$f = gh = (1)(gh) = (a_N b_M)(gh) = (b_M g)(a_N h) \tag{3}$$

But then clearly the polynomials $b_M g$ and $a_N h$ are monic, as the coefficients of the leading terms are $b_M a_N$ and $a_N b_M$ respectively, both of which are equal to 1.

Of course, this multiplication does not alter the degree, so we have produced a factorization of f into monic polynomials of strictly lesser degree.

This proves the reverse direction, so the statement holds in general. □

Exercise 2. Let p be a prime and let $\mathbb{F}_p$ be the field with p elements.

(a) List all possible ways that a monic polynomial $f \in \mathbb{F}_p[x]$ with $\deg(f) = 3$ could factor.

Proof. Ostensibly, there is one possible factorization, that is into a quadratic and linear polynomial, i.e. $f = f_1 f_2$ where f_1 is degree 2 and f_2 is degree 1.

However, there is a bit more nuance, as if/how the quadratic factors is important to the counting argument.

For this, first note that we can assume every factorization is monic (i.e. f_1, f_2 monic) without loss of generality by problem 1. With this in mind, we get 4 interesting possibilites:

(i) f_1 is irreducible

(ii) f_1 factors into two linear polynomials with roots distinct from each other and from the root of f_2

(iii) f_1 factors into two linear polynomials such that out of the now three linear polynomials in the decomposition, exactly two share the same root (i.e. multiplicity 2)

(iv) f_1 factors into linear polynomials such that the now three polynomials in the decomposition all have the same root

It is intuitively clear this describes all possibilities, as the only thing which can differ in the reducible cases is how many roots the linear polynomials in the decomposition share. □

(b) Prove that there are exactly $\frac{p^3-p}{3}$ monic, irreducible polynomials $f \in \mathbb{F}_p[x]$ with degree 3.

Proof. There are clearly p^3 possible monic degree 3 polynomials in $\mathbb{F}_p[x]$.

To find the amount of monic irreducible polynomials then, we just find the amount of monic reducible degree 3 polynomials, which can be done by counting the possible factorizations as outlined in (a).

Say then monic f is reducible and thus we have $f = f_1 f_2$ for degree 2 f_1 and degree 1 f_2. By problem 1, we can assume the factorization is monic.

(i) If f_1 is irreducible, using the hint there are $\frac{p^2-p}{2}$ choices for f_1 and clearly p choices for f_2 so we get

$$\Big(\frac{p^2-p}{2}\Big)p = \frac{p^3-p^2}{2}$$

total choices in this case.

(ii) If f_1 factors into monic linear polynomials with distinct roots, we seemingly have $p(p-1)(p-2)$ choices, but as multiplication commutes we divide this by 3!, so we get

$$\frac{p(p-1)(p-2)}{6}$$

choices in this case.

(iii) If f_1 factors into monic linear polynomials where exactly two share a root, we seemingly have $p(p-1)$ choices.

This ends up being true, as we don't need to divide here given we can write all decompositions of this form in the order of

$$(x-a)(x-a)(x-b)$$

where commuting this **does not** yield something of the same form (unlike the previous part). We thus get the amount of choices from the p choices for a and the $p-1$ choices for b, giving

$$p(p-1)$$

choices in this case.

(iv) In the case of all identical roots, there are trivially p choices.

To get the amount of reducible monic degree 3 polynomials then, we sum all these choices:

$$\frac{p^3-p^2}{2}+\frac{p(p-1)(p-2)}{6}+p(p-1)+p=\frac{2p^3+p}{3}$$

Find the amount of irreducible monic degree 3 polynomials then just comes from the difference with p^3, where we get:

$$p^3-\frac{2p^3+p}{3}=\frac{3p^3}{3}-\frac{2p^3+p}{3}=\frac{p^3-p}{3}$$

Which is the desired answer. □

(c) Conclude that there is a field of order p^3.

Proof. Note for every prime p, we have that $\frac{p^3-p}{3}\geq 1$. Thus for every p, there is a monic irreducible polynomial f in $\mathbb{F}_p[x]$ with degree 3.

We appeal then to a theorem proved in class, which has that for $K={}^{\mathbb{F}_p[x]}/_{(f)}$, we have $[K:\mathbb{F}_p]=\deg(f)=3$.

This is precisely that the dimension of K is 3 over the field $\mathbb{F}_p$, i.e. every element of K can be written uniquely as a linear combination of basis vectors with p^3 choices of coefficients.

From this it follows $|K|\leq p^3$. But each of the p^3 different linear combinations is an element of K (as it is a vector space over $\mathbb{F}_p$), so it must be $|K|\geq p^3$. It follows has precisely order p^3. □

Exercise 3. Let F and K be fields and suppose that K is an extension of F. Let $\alpha\in K$ be such that α^2 is algebraic over F. Prove that α is algebraic over F.

Proof. Assume α^2 is algebraic over F, then there exists some polynomial $f \in F[x]$ such that $f(\alpha^2) = 0$. Denote then $f = \sum_{i=0}^{N} a_i x^i$, as $f(\alpha^2) = 0$, we get the following:

$$\begin{aligned} a_N(\alpha^2)^N x^N + a_{N-1}(\alpha^2)^{N-1}x^{N-1} + ... + a_0 = 0 \\ a_N\alpha^{2N} + a_{N-1}\alpha^{2N-2} + ... + a_0 = 0 \end{aligned} \tag{4}$$

Define then the polynomial $f_2 = \sum_{i=1}^{N} a_i x^{2i}$. Clearly, $f_2 \in F[x]$, as its coefficients are just the coefficients of f, which are from F.

Moreover, (4) shows that f_2 has α as a root, so we thus have that α is algebraic over F. □

Exercise 4. Let F and K be fields and suppose that K is an extension of F. An *automorphism* of K over F is an isomorphism $\phi : K \to K$ such that $\phi(a) = a$ for every $a \in F$. Let $\mathrm{Aut}_F(K)$ be the set of automorphisms of K over F.

(a) Prove that $\mathrm{Aut}_F(K)$ is a group under the composition of functions.

Proof. We need to verify the group axioms. For this, let ϕ and ϕ be automorphisms of K over F.

(i) *(Closure under composition)* We want that $\phi \circ \psi \in \mathrm{Aut}_F(K)$. For this, recall that the composition of bijections is a bijection.

Moreover, we quickly verify $\phi \circ \psi$ is a homomorphism, as for any elements $a, b \in K$ we have

$$\phi\circ\psi(a+b) = \phi(\psi(a+b)) = \phi(\psi(a)+\psi(b)) = \phi(\psi(a))+\phi(\psi(b)) = \phi\circ\psi(a)+\phi\circ\psi(b)$$

as well as

$$\phi \circ \psi(ab) = \phi(\psi(ab)) = \phi(\psi(a)\psi(b)) = \phi(\psi(a))\phi(\psi(b)) = \phi \circ \psi(a)\phi \circ \psi(b),$$

and so $\phi \circ \psi$ is an isomorphism. We just want to check $\phi \circ \psi$ fixes F then, which we see as for $c \in F$ we have

$$\phi \circ \psi(c) = \phi(\psi(c)) = \phi(c) = c,$$

and so we have closure under the composition of functions.

(ii) *(Existence of an Identity)* We want to verify there is an identity element.

We purport this should be the trivial automorphism given by the identity function, i.e. the $\mathbb{1} : K \to K$ for which $\phi(a) = a$ for all $a \in K$.

It is trivial that this function is in $\mathrm{Aut}_F(K)$, as the identity is clearly an isomorphism and it of course fixes F.

Moreover, it is clear that composition with the identity function just returns the original function, and so the identity function is our identity element.

(iii) *(Associativity of Composition)* We just recall the composition of functions in general is associative.

(iv) *(Existence of Inverses)* Clearly, ϕ admits a bijective inverse ϕ^{-1} as it is a bijection. We need to verify then that $\phi^{-1} \in \mathrm{Aut}_F(K)$.

We want first to show then that ϕ^{-1} is a homomorphism. For this, we define $c = \phi^{-1}(a+b)$. It follows $\phi(c) = a + b$, but as ϕ is a surjection $K \to K$, we have that $a = \phi(d), b = \phi(e)$ given $d, e \in K$.

Thus $\phi(c) = \phi(d) + \phi(e) = \phi(d + e)$. Using that ϕ is an injection, then we have $c = d + e$, but also $d = \phi^{-1}(a)$ and $e = \phi^{-1}(b)$.

Combining these facts then has $\phi^{-1}(a + b) = \phi^{-1}(a) + \phi^{-1}(b)$. Essentially the exact same argument proceeds for multiplication, so we conclude ϕ^{-1} is an automorphism of K.

Moreover, as $\phi(c) = c$ for $c \in F$, applying ϕ^{-1} to both sides gets $c = \phi^{-1}(c)$, so ϕ^{-1} still fixes F. Thus $\phi^{-1} \in \mathrm{Aut}_F(K)$.

It follows $\mathrm{Aut}_F(K)$ is a group under the composition of functions. □

(b) If $\alpha \in K$ is algebraic over F, prove that $\phi(\alpha)$ is also algebraic over F for every $\phi \in \mathrm{Aut}_F(K)$.

Proof. Let $\alpha \in K$ such that α is algebraic over F, that is there is a polynomial $f = \sum_{i=0}^{N} a_i x^i \in F[x]$ such that $f(\alpha) = 0$. Note then

$$\phi\Big(\sum_{i=0}^{N} a_i \alpha^i\Big) = \phi(0) = 0 \tag{5}$$

as group homomorphisms send the additive identity to the additive identity. Using that $a_i \in F$ for all i then and that ϕ fixes elements in F, we get

$$0 = \phi\Big(\sum_{i=0}^{N} a_i \alpha^i\Big) = \sum_{i=0}^{N} \phi(a_i \alpha^i) = \sum_{i=0}^{N} \phi(a_i)\phi(\alpha)^i = \sum_{i=0}^{N} a_i \phi(\alpha)^i = f(\phi(\alpha)), \tag{6}$$

which shows that $\phi(a)$ is also a root of $f \in F[x]$, and so it algebraic over F. □

(c) Find $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(i)), \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$ and $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$.

Proof. In Homework #2, we showed the only possible *homomorphisms* $\mathbb{Q}(i) \to \mathbb{Q}(i)$ are the automorphisms given by the identity and conjugation mappings.

Clearly, both of these mappings fix $\mathbb{Q}$, so $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(i))$ is just the group consisting of the identity mapping and conjugation mapping, i.e. $\cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.

For finding $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$, we let ϕ be an automorphism of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. We want to determine the value $\phi(\sqrt[3]{2})$, which can done in the following way:

$$\begin{aligned} \phi(\sqrt[3]{2}^3 - 2) = \phi(0) = 0 \to \phi(\sqrt[3]{2}^3) - \phi(2) = 0 \\ \to \phi(\sqrt[3]{2})^3 - 2 = 0 \to \phi(\sqrt[3]{2})^3 = 2 \\ \to \phi(\sqrt[3]{2}) = \sqrt[3]{2} \end{aligned} \tag{7}$$

This implies then that ϕ must be the identity mapping, as for $a + b\sqrt[3]{2}$ we get using the established properties of ϕ that

$$\phi(a + b\sqrt[3]{2}) = \phi(a) + \phi(b)\phi(\sqrt[3]{2}) = a + b\sqrt[3]{2} \tag{8}$$

So $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$ just consists of the identity mapping, i.e. it is isomorphic to the trivial group.

For $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$, we do the exact same work as the previous example, except with $i^2 + 1$. Doing this shows that $\phi(i)$ must be a root of $x^2 + 1$, i.e. it is either i or $-i$.

This of course clearly shows any given automorphism of $\mathbb{C}$ over $\mathbb{R}$ is either the identity mapping or the conjugation mapping, as seen in (8).

Thus $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ is the group of the identity and conjugation map, i.e. $\cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. □