David O.H. Cutler

Math 146: Homework 6

April 8, 2024

Exercise 1. Let $a \in \mathbb{Z}$ be non-zero and not a perfect cube, and let $f \in \mathbb{Q}[x]$ be given by $f = x^3 - a$.

(a) Prove that f is irreducible.

Proof. Recall we have that f is irreducible over $\mathbb{Q}$ if it it is "irreducible over $\mathbb{Z}$", i.e. it can't factor into integer-coefficient polynomials with strictly lesser degree.

Moreover, as f is cubic, it having no solutions is strong enough to imply its irreducibility. By the previous reasoning then, it is strong enough to verify it has no solutions in $\mathbb{Z}$.

This however is true by assumption as we stipulated a is not a perfect cube, as so there it cannot be there is an integer solution to $f = x^3 - a$. Thus f is irreducible. □

(b) Prove that the splitting field L of f over $\mathbb{Q}$ is $L = \mathbb{Q}(\sqrt[3]{a}, \sqrt{-3})$, and that $[L : \mathbb{Q}] = 6$.

Proof. By the hint, we determine quickly the three solutions f in $\mathbb{C}$ are

$$x = \sqrt[3]{a}, \sqrt[3]{a}\frac{-1+\sqrt{-3}}{2}, \sqrt[3]{a}\frac{-1-\sqrt{-3}}{2},$$

and so we form the splitting field of f by iteratively appending roots to get

$$\mathbb{Q}\Big(\sqrt[3]{a}, \sqrt[3]{a}\frac{-1+\sqrt{-3}}{2}, \sqrt[3]{a}\frac{-1-\sqrt{-3}}{2}\Big),$$

i.e. the *smallest* field containing all the roots of f and $\mathbb{Q}$. We want to show then this corresponds with $\mathbb{Q}(\sqrt[3]{a}, \sqrt{-3})$. Note first

$$\Big(2\Big(\sqrt[3]{a}\frac{-1+\sqrt{-3}}{2}\Big) + \sqrt[3]{a}\Big)\sqrt[3]{a}^{-1} = \sqrt{-3}$$

so the former field must contain $\sqrt{-3}$ (note all of the elements used are *a priori* in $\mathbb{Q}(\sqrt[3]{a}, \sqrt{-3})$). It clearly also contains $\sqrt[3]{a}$, so as the latter field is the smallest field containing $\mathbb{Q}$ and these additional elements, we must have:

$$\mathbb{Q}(\sqrt[3]{a}, \sqrt{-3}) \subseteq \mathbb{Q}\Big(\sqrt[3]{a}, \sqrt[3]{a}\frac{-1+\sqrt{-3}}{2}, \sqrt[3]{a}\frac{-1-\sqrt{-3}}{2}\Big).$$

We similarly have the other inclusion, as we can trivially form all of the adjoined roots using elements in $\mathbb{Q}(\sqrt[3]{a}, \sqrt{-3})$ and apply the same reasoning. Thus the splitting field L is $\mathbb{Q}(\sqrt[3]{a}, \sqrt{-3})$.

With this in mind then, note we can say

$$L = \mathbb{Q}(\sqrt[3]{a}, \sqrt{-3}) \cong \frac{\Big(\mathbb{Q}[x]/(x^3-a)\Big)[y]}{(y^2+3)} \cong \frac{\mathbb{Q}(\sqrt[3]{a})[y]}{(y^2+3)},$$

where these quotients are representing our adjoining of roots. Note this construction is valid as y^2+3 is irred. over ${}^{\mathbb{Q}[x]}/_{(x^3-a)} \cong \mathbb{Q}(\sqrt[3]{a})$ as $\mathbb{Q}(\sqrt[3]{a}) \subseteq \mathbb{R}$, in which the square of all elements is non-negative.

By the degree formula then we note

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt[3]{a})][\mathbb{Q}(\sqrt[3]{a}):\mathbb{Q}] = 3 \cdot 2,$$

where these degrees follows the quotients we outlined. Thus $[L:\mathbb{Q}] = 6$. □

(c) Prove that $\mathrm{Gal}(f) \cong S_3$.

Proof. Recall we have an embedding $\mathrm{Gal}(f) \hookrightarrow S_{\deg(f)}$ given by an injective homomorphism ϕ, i.e. $\mathrm{Gal}(f)$ is isomorphic to a subgroup of $S_{\deg(f)}$. In this case, the embedding is into S_3.

As we have $[L:\mathbb{Q}] = 6$, we know furthermore $|\mathrm{Gal}(f)| = 6$ (as the roots of f are distinct). Of course $|S_3| = 3! = 6$, so we have an injection ϕ between two sets of the same cardinality. It follows ϕ is a surjection.

Thus ϕ is an isomorphism mapping, and we have $\mathrm{Gal}(f) \cong S_3$. □

Exercise 2. Let p be a prime.

(a) Prove that every polynomial $f \in \mathbb{F}_p[x]$ with degree 2 splits completely in $\mathbb{F}_{p^2}$.

Proof. Let $f \in \mathbb{F}_p[x]$ with degree 2. If f is reducible over $\mathbb{F}_p$, then it automatically splits in $\mathbb{F}_{p^2}$.

Say then it is irreducible; we can assume without loss of generality it is monic as scaling by a constant does not affect whether or not the polynomial splits.

By the previous homework, f has two roots in $\mathbb{F}_{p^2}$, say α and β, the minimal polynomial in $\mathbb{F}_{p^2}[x]$ of which are

$$(x-\alpha), (x-\beta).$$

Following the mechanics in Problem 3 (b.) then, we note

$$f = (x-\alpha)(x-\beta),$$

i.e. f splits, as desired. □

(b) Let $\alpha \in \mathbb{F}_{p^3}$, and suppose α is not an element of $\mathbb{F}_p$. Prove that α is a root of some monic, irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree 3.

Proof. Note $[\mathbb{F}_{p^3} : \mathbb{F}_p] = 3$, i.e. it is a finite extension. Therefore it is algebraic, and so we can consider the minimal polynomial f of α over $\mathbb{F}_p$.

We know $|\deg(f)| \leq [\mathbb{F}_{p^3} : \mathbb{F}_p] = 3$ (in particular, I gave a proof of this fact on the last homework), moreover, we know the minimal polynomial cannot be linear, as this would trivially have $\alpha \in \mathbb{F}_p$.

The concerning case thus is that the minimal polynomial is degree 2.

However, we note this cannot be the case as we showed on the previous homework that the roots of degree 2, monic, irreducible polynomials over $\mathbb{F}_p$ are exclusively accounted for by elements of $\mathbb{F}_{p^2}$.

Moreover, we also showed that $\mathbb{F}_{p^3}$ is not an extension of $\mathbb{F}_{p^2}$. Putting these facts together, we see clearly that it cannot be that the minimal polynomial is quadratic, as it would thus contradict the fact that $\mathbb{F}_{p^3}$ does not extend $\mathbb{F}_{p^2}$.

In particular, this would have $\alpha \in \mathbb{F}_{p^2}$, which would force

$$\mathbb{F}_{p^3} \supseteq \mathbb{F}_p(\alpha) = {}^{\mathbb{F}_p[x]}/_{(f)} = \mathbb{F}_{p^2},$$

which as we said is not a possibility.

Thus the only possibility is our minimal polynomial is degree 3. It of course has α as a root, and it is furthermore monic and irreducible, as desired. □

(c) Prove that every irreducible degree 3 polynomial in $\mathbb{F}_p[x]$ splits completely in $\mathbb{F}_{p^3}$.

Proof. Recall we have $\frac{p^3-p}{3}$ monic, irreducible polynomials of degree 3. Moreover, we have $p^3 - p$ elements in $\mathbb{F}_{p^3} \setminus \mathbb{F}_p$.

Using a pigeonhole argument on the mapping that sends elements in $\mathbb{F}_{p^3}$ to the unique monic, irreducible, degree 3 polynomials they are roots of, we get that each monic, irreducible, degree 3 polynomial has exactly 3 distinct roots in $\mathbb{F}_{p^3} \setminus \mathbb{F}_p$.

(I outlined this exact proof idea in much more detail on the last homework, so I am treating it as an established motif. If anything is unclear, please reference that.)

Consider without loss of generality an arbitrary *monic*, irreducible, degree 3 polynomial f over $\mathbb{F}_p$ then and label its three roots in $\mathbb{F}_{p^3} \setminus \mathbb{F}_p$ as $\alpha_1, \alpha_2, \alpha_3$.

The minimal polynomials corresponding to these roots in $\mathbb{F}_{p^3}$ are of the course the linear polynomials given by

$$x - \alpha_1, x - \alpha_2, x - \alpha_3.$$

Following the mechanics outlined in Problem 3 (b.) then, we conclude

$$f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3),$$

i.e. f splits completely over $\mathbb{F}_{p^3}$. □

(d) Does every degree 3 polynomial in $\mathbb{F}_p[x]$ split completely completely over $\mathbb{F}_{p^3}$?

Proof. No. Assume for contradiction this was the case; take an arbitrary degree 2, monic, irreducible $f \in \mathbb{F}_p[x]$.

Then xf is a degree 3 polynomial over $\mathbb{F}_p$, by hypothesis we have for some $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{p^3}$ that

$$xf = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

Applying **Euclid's Lemma** trivially shows then at least one α must be zero (i.e. note x the right side), for example

$$xf = x(x - \alpha_2)(x - \alpha_3).$$

As $\mathbb{F}_{p^3}[x]$ is an integral domain, we can cancel to get

$$f = (x - \alpha_2)(x - \alpha_3),$$

i.e. f splits over $\mathbb{F}_{p^3}$. Recall then the splitting field of f is the smallest field over which f splits linearly.

We've just shown it does so over $\mathbb{F}_{p^3}$, and we showed earlier it does over $\mathbb{F}_{p^2}$. Thus the splitting field is a subfield of both, so its order must divide both p^2 and p^3 by applying **Lagrange's Theorem** over the underlying additive groups.

Recall then only prime powers divide prime powers, so the only options for the order of the splitting field are p and p^2.

Of course, the splitting field cannot be the field with p^2 elements, as this would have $\mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^3}$, which we showed on a previous homework to be impossible.

Moreover, it cannot be that the splitting field is the field with p elements, as we as assumed f was irreducible over $\mathbb{F}_p$, and so it doesn't split. Thus we have reached a contradiction, and so it cannot be that all degree 3 polynomials split. □

Exercise 3. Let p be a prime and let $q = p^k$ for some integer $k \geq 1$.

(a) Prove that every element of $\mathbb{F}_q$ is a root of the polynomial $x^q - x \in \mathbb{F}_p[x]$, with multiplicitly 1.

Proof. Note we have

$$x^q - x = x(x^{q-1} - 1)$$

Recall then that $\mathbb{F}_q^\times$ is cyclic, i.e. we have that each element $\alpha \in \mathbb{F}_q^\times$ is order $q-1$, that is $\alpha^{q-1} = 1$. It trivially follows each $\alpha \in \mathbb{F}_q^\times$ is a root of $x^q - x$ by the given equation.

Moreover, 0 is also clearly a root as we get $0(0-1) = 0$. It follows all elements of $\mathbb{F}_q$ are roots of $x^q - x$.

Recall then additionally, given that $\mathbb{F}_q$ is an extension of $\mathbb{F}_p$, we have that the roots of $x^q - x$ in $\mathbb{F}_q$ counted with multiplicitly are bounded by the degree of the polynomial, which is q.

Thus the only possibility is each root has multiplicitly 1, as we already have q roots. □

(b) In fact, prove that if we consider it in the ring $\mathbb{F}_q[x]$, the polynomial $x^q - x$ splits completely as

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$$

Proof. Recall that if $f, g, h \in F[x]$ are such that $f|h$ and $g|h$ with $\gcd(f, g) = 1$, then we have $fg|h$ as a direct consequence of **Bézout's Identity**.

Moreover, recall that the minimal polynomial of a root α divides any polynomial with α as a root.

As distinct minimal polynomials are irreducible then, they must be coprime, so their product must thus divide anything which the two roots corresponding to these minimal polynomials.

We note this argument generalizes to any such product of minimal polynomials (in particularly, linear ones) as we are working in a UFD with irreducibles as our prime elements; for instance if we have distinct roots $\alpha_1, \alpha_2, \alpha_3$ we must have

$$\gcd((x - \alpha_1)(x - \alpha_2), (x - \alpha_3)) = 1,$$

appealing to our unique factorization. One remarks this generalizes inductively.

Note then the minimal polynomials corresponding to the roots of $x^q - x$ in $\mathbb{F}_q[x]$ are trivially just $\{x - \alpha \mid \alpha \in \mathbb{F}_q\}$, as each root α of $x^q - x$ is in $\mathbb{F}_q$. By our earlier reasoning then

$$\prod_{\alpha \in \mathbb{F}_q} (x - \alpha) \Big| x^q - x,$$

i.e. the product divides.

Moreover, this product is monic, and of degree q. So we have a monic, degree q polynomial dividing $x^q - x$. Clearly then, the only possibility is that

$$\prod_{\alpha \in \mathbb{F}_q} (x - \alpha) = x^q - x,$$

as desired. □

(c) Prove that if $f \in \mathbb{F}_p[x]$ is an irreducible factor of $x^q - x$ in $\mathbb{F}_p[x]$, then the degree of f is at most k.

Proof. Remark that $\mathbb{F}_q$ is *the* splitting field of $x^q - x$; not just because we showed that $x^q - x$ splits completely over $\mathbb{F}_q$, but because $\mathbb{F}_q$ is precisely $\mathbb{F}_p$ adjoined with the roots of $x^q - x$ (recall the roots are just $\mathbb{F}_q$).

Recall then how we construct the splitting field of $x^q - x$; we factor $x^q - x$ into irreducible factors, quotient about by any nonlinear irreducible factor, and refactor over the new field that is generated.

Say then we factor $x^q - x$ into irreducible factors as

$$x^q - x = fgh...,$$

(assuming at least one, f, is nonlinear; otherwise the statement is automatically true) where we intend to show that the arbitrary f in particular has degree at most k.

One iteration of this process generates a chain of fields

$$\mathbb{F}_p \subseteq {}^{\mathbb{F}_p[x]}/_{(f)} \subseteq K_2 \subseteq ... \subseteq K_{q-1} \subseteq \mathbb{F}_q,$$

so we get the expansion with the degree formula given by

$$k = [\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_q : K_{q-1}]...[K_2 : {}^{\mathbb{F}_p[x]}/_{(f)}][{}^{\mathbb{F}_p[x]}/_{(f)} : \mathbb{F}_p],$$

but we know $[{}^{\mathbb{F}_p[x]}/_{(f)} : \mathbb{F}_p] = \deg(f)$. As each degree then ≥ 1 and we have the product is k, it follows $\deg(f)$ is bounded by k, as desired. □

(d) Describe completely how the polynomials $x^p - x, x^{p^2} - x$, and $x^{p^3} - x$ factor in $\mathbb{F}_p[x]$.

Proof. Trivially, we know that $x^p - x$ splits linearly into the product $\prod_{\alpha \in \mathbb{F}_p} (x - \alpha)$ by our previous work.

For $x^{p^2} - x$ note we have all elements of $\mathbb{F}_{p^2}$ as roots. The subset of these in $\mathbb{F}_p$ exhaustively gets all monic linear polynomials in the factorization of $x^p - x$, whereas those in the difference characterize all monic, irreducible polynomials of degree 2, as seen in Problem 2.

Thus $x^{p^2} - x$ factors into the product of all monic, linear polynomials over $\mathbb{F}_p$ and all degree 2, monic, irreducible polynomials over $\mathbb{F}_p$.

Similar reasoning holds exactly for $x^{p^3} - x$ as seen in Problem 2; we get $x^{p^3} - x$ as the product of all monic, linear polynomials over $\mathbb{F}_p$ and all degree 3, monic, irreducible polynomials over $\mathbb{F}_p$. $\square$