# Math 404 HW 6 Solutions

## 1 Problem 6.1

Determine the splitting fields $\mathbb{Q} \subset K$ of the following polynomials defined over $\mathbb{Q}$ and compute the degree $|K : \mathbb{Q}|$.

(a) $f(x) = x^4 + 1$

(b) $f(x) = x^3 - 3x + 2$.

For (b), note that $f = (x-1)^2(x+2)$, so the splitting field is just $\mathbb{Q}$ itself, with degree 1. So we just answer (a).

*Proof.* I claim that $K = \mathbb{Q}(\sqrt{i})$, and $|K : \mathbb{Q}| = 4$. We may also write $K = \mathbb{Q}(\sqrt{2}, i)$, but we won't be writing up a solution in that vein.

To see this, let $\alpha$ be a root of $f$. Then the roots of $f$ are $\pm\alpha, \pm i\alpha$. But note that since $\alpha^4 = -1$, we have that $\alpha^2 = \pm i$. Let's say without loss of generality that $\alpha = \sqrt{i}$. Thus we have that the roots of $f$ are $\pm\alpha, \pm\alpha^3$. This shows that all the roots of $f$ live in $\mathbb{Q}(\sqrt{i})$. That is, we have that $K \subset \mathbb{Q}(\sqrt{i})$, and the reverse containment holds because $\sqrt{i}$ is a root of $f$.

For the degree statement, consider the chain of fields $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(\sqrt{i})$. The first extension is of degree 2 by standard arguments. The second extension will be of degree 2 provided we can show that $\sqrt{i} \notin \mathbb{Q}(i)$, and then the multiplicative property of the degree will yield the desired result.

For this, suppose towards a contradiction that we have $z^2 = i$ for some $z \in \mathbb{Q}(i)$. Then we may uniquely write $z = a + bi$ for $a, b \in \mathbb{Q}$. Then we have

$$i = z^2 = a^2 - b^2 + 2abi.$$

Linear independence of 1 and $i$ over $\mathbb{Q}$ yields the equalities

$$\begin{aligned} 0 &= a^2 - b^2 \\ 1 &= 2ab. \end{aligned}$$

The second equality yields that neither $a$ nor $b$ are zero, and that $b = \frac{1}{2a}$. Plugging this into the first equality and rearranging yields $a^4 = 1/4$ so $a^2 = \pm 1/2$, so $(1/a)^2 = \pm 2$. This yields that $\sqrt{\pm 2}$ is rational, which is false. Thus, we must have that $\sqrt{i} \notin \mathbb{Q}(i)$, and the result holds. □

As a remark, the computations at the end here show that$\sqrt{i} = \frac{1}{\sqrt{2}}(1+i)$, which can be used to get the alternate description $K = \mathbb{Q}(\sqrt{2}, i)$. Which form you choose is a matter of aesthetic taste.

## 2 Problem 6.2

(a) Show that $\mathbb{Q}(\sqrt{2}, i)$ is the splitting field of $f(x) = x^2 - 2\sqrt{2}x + 3$ over $\mathbb{Q}(\sqrt{2})$.

(b) Find a polynomial $f(x) \in \mathbb{Q}[x]$ whose splitting field is $\mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3})$.

(a) Let $K$ be the splitting field of $f$. We compute the roots of $f$ using the quadratic formula as

$$\alpha_\pm = \sqrt{2} \pm i.$$

This shows that all the roots of $f$ are elements of $\mathbb{Q}(\sqrt{2}, i)$, so by minimality we get $K \subseteq \mathbb{Q}(\sqrt{2}, i)$. For the reverse containment, note that since $\alpha_+$ and $\alpha_0$ are in $K$, we have that

$$i = \frac{\alpha_+ - \alpha_-}{2} \in K,$$

so by minimality we have $\mathbb{Q}(\sqrt{2}, i) \subseteq K$ and equality holds, as desired.

□

(b) Ideally we'd want at least to have that $f(\sqrt[3]{2}) = f(i) = 0$. Then by definition of minimal polynomials, we'd have that $g(x) := (x^3 - 2)(x^2 + 1)$ divides $f$ (this follows from the fact that the roots of these two polynomials are disjoint). I claim that the splitting field of $g$ is the desired field.

To see this, let $K$ be the splitting field of $g$, and let $L = \mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3})$. Note that the roots of $g$ are

$$\pm i, \ \sqrt[3]{2}, \ \text{and} \ \sqrt[3]{2}\left(\frac{-1}{2} \pm i\frac{\sqrt{3}}{2}\right),$$

which are all evidently elements of $L$. Since $K$ is the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and the roots of $g$, we get $K \subset L$. For the reverse containment, note that since $i$ and $\sqrt[3]{2}$ are in $K$, we have that

$$\sqrt{3} = \frac{\sqrt[3]{2}\left(\frac{-1}{2} + i\frac{\sqrt{3}}{2}\right) - \sqrt[3]{2}\left(\frac{-1}{2} - i\frac{\sqrt{3}}{2}\right)}{2\sqrt[3]{2}i} \in K.$$

Thus, by minimality of $L$, we have that $L \subset K$, and equality holds, as desired. Similar reasoning would also have worked with $(x^3-2)(x^2-3)$.

$\square$

# 3 Problem 6.3

Let $K$ be a field and let $L = K(\alpha)$ be a simple field extension of $K$. If $L$ is normal over $K$, show that $L$ is the splitting field of the minimal polynomial of $\alpha$.

*Proof.* Let $f(x) \in K[x]$ be the minimal polynomial for $\alpha$. Since $f$ is irreducible, has one root in $L$, and $L$ is normal, we have that $f$ splits in $L$. Since $L$ is generated over $K$ by just the one root of $f$, it is also generated by all the roots of $f$. The conclusions of the previous two sentences are the defining properties of the splitting field for $f$, so $L$ is the splitting field for $F$, as desired. □

# 4 Problem 6.4

(a) Count the number of monic irreducible polynomials over $\mathbb{F}_3$ of degree 2, 3, and 4.

(b) For each $d = 2, 3, 4$, explicitly exhibit a monic irreducible polynomail $f \in \mathbb{F}_3[x]$ of degree $d$.

Throughout this problem, for any finite set $X$, we will let $\#X$ denote the number of elements in $X$. For any $d$ let $I_d$ denote the set of irreducible polynomials of degree $d$ in $\mathbb{F}_3[x]$. I claim

$$\#I_2 = 3$$
$$\#I_3 = 8$$
$$\#I_4 = 18$$

this answers (a), and we will see 3 ways to get at this answer below.

For (b), I claim that $x^2 + 1, x^3 - x + 1$, and $x^4 + x - 1$ are all irreducible. The first two can be verified by checking they have no roots. The third can be verified to have no roots. So after checking that $x^2 + 1, x^2 + x - 1$, and $x^2 - x - 1$ are all the irreducible monic quadratics, we can verify that $x^4 + x - 1$ is irreducible by shwoing that none of these irreducible monic quadratics divide it. The rest of this solution is dedicated to three ways of solving (a).

## 4.1 Algorithmic solution

One approach is to algorithmically produce a list of all monic irreducible polynomials of a given degree given knowledge of monic irreducible polynomials of smaller degree, where we can show that a monic polynomial is irreducible by checking via division with remainder if it is divisible by smaller degree monic irreducibles. And indeed for degrees 2 and 3, we just need to check divisibility by the linear polynomials, which is just whether or not they have a root. For degree 4 we need to check for roots and divisibility by the 3 irreducible monic degree 2 polynomials. I will not be writing up the details of this approach, though it works just fine, and has the added benefit of producing a list of irreducible polynomials as you go. The downside is there's quite a lot of tedium, some of which can be diminished using the PolynomialRemainder function in Mathematica, and then reducing the remainder it gives you mod 3.

## 4.2 Leveraging finite field properties

In my opinion the most elegant way to compute this is to prove that for any prime $p$ and positive integer $n$ that $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ factors as the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of degrees dividing $n$.

Indeed, if we have an irreducible polynomial $g$ dividing $f$, then we may consider the field $L = \mathbb{F}_p[x]/(g)$. Since $f$ splits in $\mathbb{F}_{p^n}$, so does $g$. In particular, there is some root of $g$ in $\mathbb{F}_{p^n}$, so picking one of these roots yields a chain of field extensions $\mathbb{F}_p \subset L \subset \mathbb{F}_{p^n}$. The multiplicative property of the degree yields that $|L : \mathbb{F}_p| = \deg g$ divides $|\mathbb{F}_{p^n} : \mathbb{F}_p| = n$. So every irreducible factor of $f$ has degree dividing $n$. Showing that any irreducible polynomial of degree dividing $n$ divides $f$ amounts to more or less reversing this reasoning using some splitting field trickery.

Counting degrees in this factorization of $f$ as the product of all monic irreducible polynomials of degree dividing $n$ yields

$$p^n = \sum_{d|n} d \cdot \#I_d.$$

Starting with the direct computation $\#I_1 = p$ (the monic irreducible linear polynomials are just $x - \alpha$ for $\alpha \in \mathbb{F}_p$), this yields a recursive formula for $\#I_d$ given $\#I_c$ with $c < d$. For instance, we have

$$p^2 = 1 \cdot \#I_1 + 2 \cdot \#I_2 = p + 2\#I_2,$$

so $\#I_2 = (p^2 - p)/2$. In the case $p = 3$, this yields $\#I_2 = 3$, as we claimed.

We also compute

$$3^3 = 1 \cdot \#I_1 + 3 \cdot \#I_3 = 3 + 3 \cdot \#I_3.$$

Solving this yields $\#I_3 = 8$.

Finally we have

$$\begin{aligned} 3^4 &= 1 \cdot \#I_1 + 2 \cdot \#I_2 + 4 \cdot \#I_4 \\ &= 3 + 6 + 4 \cdot \#I_4, \end{aligned}$$

so $\#I_4 = 18$.

$\square$

## 4.3 Combinatorial proof

There is a third option sitting in between the two above ideas, which is to simply count the outputs of the algorithm described in the first method. To do this, let $P_d$ denote the set of monic polynomials of degree $d$ in $\mathbb{F}_3$, and let $R_d$ denote the set of reducible monic polynomials of degree $d$. So we have the basic relationship

$$\#I_d = \#P_d - \#R_d.$$

Furthermore, we have $\#P_d = 3^d$ (we can choose from any of three possible coefficients for the $d$ nonleading terms, and we pick 1 for the leading term). Thus, we reduce the problem of determining $I_d$ to determining $R_d$. And we can split up the count of $R_d$ by the degrees of polynomials appearing in decomposition into monic irreducibles, so we can determine $R_d$ given knowledge of $I_c$ for $c < d$.

We can start off the count with $\#I_1 = 3$, that there are three monic irreducible degree 1 polynomials over $\mathbb{F}_3$. So for $I_2$, we have

$$\begin{aligned}\#I_2 &= 3^2 - \#R_2 \\ &= 9 - \#\{L_1 \cdot L_2 : L_i \in I_1\}.\end{aligned}$$

To count this last set, we need a small lemma, which you may have seen before, but I'm including here for reference.

**Lemma 1.** *Let $X$ be a set of size $n$. Then the number of ways of picking $k$ elements out of $X$ without distinguishing the order in which they are picked and allowing repetition is*

$$\binom{n+k-1}{k}.$$

We will give a proof of this lemma at the end, but before doing so we'll see how we can use it to finish up the count.

We had shown above that

$$\#I_2 = 9 - \#\{L_1 \cdot L_2 : L_i \in I_1\}.$$

Since $\#I_1 = 3$, this latter set is obtained by picking two elements out of the size 3 set $I_1$ without order and with repition allowed. That is, we have

$$\#I_2 = 9 - \binom{3+2-1}{2} = 9 - \binom{4}{2} = 9 - 6 = 3.$$

Similarly, since any reducible cubic is either the product of three linear polynomials or a linear polynomial and an irreducible quadratic, we get

$$\begin{aligned}\#I_3 &= \#P_3 - \#R_3 \\ &= 3^3 - \Big(\#\{L_1L_2L_3 : L_i \in I_1\} + \#\{L \cdot Q : L \in I_1 \text{ and } Q \in I_2\}\Big) \\ &= 27 - \left(\binom{3+3-1}{3} + \#I_1 \cdot \#I_2\right) \\ &= 27 - (10 + 3 \cdot 3) \\ &= \boxed{8}.\end{aligned}$$

Any reducible degree 4 polynomial is either the product of 4 linear polynomials, the product of 2 linear polynomials and an irreducible quadratic, the product of 1 linear polynomial and an irreducible cubic, or the product of two irreducible quadratics. This yields

$$\begin{aligned}\#R_4 = {}& \#\{L_1L_2L_3L_4 : L_i \in I_1\} + \#\{L_1L_2Q : L_i \in I_1 \text{ and } Q \in I_2\} \\ &+ \#\{LC : L \in I_1 \text{ and } C \in I_3\} + \#\{Q_1Q_2 : Q_i \in I_2\} \\ ={}& \binom{3+4-1}{4} + \binom{3+2-1}{2} \cdot 3 + 3 \cdot 8 + \binom{3+2-1}{2} \\ ={}& 63.\end{aligned}$$

Thus, we have

$$\#I_4 = \#P_4 - \#R_4 = 3^4 - 63 = \boxed{18},$$

as desired.

*Proof. Proof of lemma (1)*

One way I like to think about this is to think of $X$ as the set of $n$ flavors of soda you can buy at a vending machine, and we're trying to count the number of ways to fill up a shopping cart with $k$ sodas. The argument that follows is often called a "stars and bars" argument.

One way you could think about listing all the possibilities out is to order the flavors somehow (maybe top left in the vending machine down to bottom right), and think about creating a tally for each of the flavors in order. To do this, you could write down $n-1$ separators $|$, to separate the tally for each flavor from the one before and after (think, if you have 2 flavors you'd only need 1 separator, if you have 3 flavors you'd need 2 separators, etc.). Then you could just fill up this tally with *'s between the the $|$'s, producing something like the following for $n=3$ and $k=6$

$$\begin{gathered} * * \mid * * * \mid *, \\ * \mid * \mid * * * * \end{gathered}$$

where the first row corresponds to 2 of the first type, 3 of the second, and 1 of the third. The second row would be 1 of the first and second types and 4 of the third. The key feature is that in all of these counts, you have $k$ stars corresponding to the $k$ sodas you picked, and $n-1$ separators. So no matter what you'll have $n+k-1$ symbols written down. And actually if you just keep track of which of these $n+k-1$ symbols are the $k$ stars, you could just fill in the rest of the symbols as bars.

That is, we have established a bijection between fillings of a shopping cart with $k$ sodas from $n$ flavors and subsets of size $k$ from the set of $n+k-1$ symbol positions. Since there are $\binom{n+k-1}{k}$ such subsets, the result holds $\square$

## 5 Problem 6.5

For each of the following field extensions, determine (a) whether it is normal and (b) whether it is separable.

(a) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{-5})$

(b) $\mathbb{Q}(i) \subset \mathbb{Q}(i, \sqrt[3]{2})$

(c) $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ where $p$ is a prime.

(d) $\mathbb{F}_p(x^p) \subset \mathbb{F}_p(x)$ where $p$ is a prime.

(a) This extension is both normal and separable. It is separable as $\mathbb{Q}$ has characteristic zero. It is normal as $\mathbb{Q}(\sqrt{-5})$ is the splitting field of $x^2 + 5$, and splitting fields are normal (proven in lecture).

(b) This extension is separable but not normal. It is separable because $\mathbb{Q}(i)$ has characteristic zero. To see that is is not normal, consider the polynomial $f(x) = x^3 - 3$. I claim that $f$ is irreducible over $\mathbb{Q}(i)$, but that it has only one root in $\mathbb{Q}(\sqrt[3]{2}, i)$. Showing this will prove that the extension is not normal.

First we show that $f$ is irreducible over $\mathbb{Q}(i)$. Since $f$ is of degree 3, it suffices to show that $f$ has no roots in $\mathbb{Q}(i)$. The roots of $f$ are

$$\sqrt[3]{2}, \quad \frac{\sqrt[3]{2}}{2}(-1 + \sqrt{3}i), \text{ and } \frac{\sqrt[3]{2}}{2}(-1 - \sqrt{3}i).$$

The elements of $\mathbb{Q}(i)$ may all be written uniquely in the form $a + bi$ with $a, b \in \mathbb{Q}$. Since $\sqrt[3]{2} \notin \mathbb{Q}$ (say by Eisenstein on $x^3 - 2$) and 1 and $i$ are linearly independent over $\mathbb{R}$, none of the above elements have this form, so none of them live in $\mathbb{Q}(i)$, and $f$ is irreducible.

Now it just remains to show that nonreal roots of $f$ are not in $\mathbb{Q}(\sqrt[3]{2}, i)$. Indeed, if either of the nonreal roots of $f$ were in this field, then similar algebra to that in problem 2 (b) would yield that $\sqrt{3}$ is in this field. But then we would have a chain of fields

$$\mathbb{Q}(i) \subset \mathbb{Q}(i, \sqrt{3}) \subset \mathbb{Q}(i, \sqrt[3]{2})$$

Since $\sqrt{3} \notin \mathbb{Q}(i)$ the first extension is of degree 2. Then by the multiplicative property of the degree, we would have that 2 divides $|\mathbb{Q}(i, \sqrt[3]{2}) : \mathbb{Q}(i)|$. However $f$ is irreducible, it is the minimal polynomial for $\sqrt[3]{2}$ over $\mathbb{Q}(i)$, we have that $|\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(i)| = 3$. Thus, we have that 2 divides 3, which is false. Thus, our assumption that $\mathbb{Q}(\sqrt[3]{2}, i)$ contained one of the nonreal roots of $f$ must not hold, as desired. □

(c) First, two lemmas

**Lemma 2.** *Let $R$ be a commutative ring where a prime number $p$ is zero in $R$. Then the map $\varphi : R \to R$ defined by $\alpha \mapsto \alpha^p$ is a homomorphism, called the <u>Frobenius</u> homomorphism.*

*Proof.* We compute

$$\begin{aligned}\varphi(\alpha+\beta) &= (\alpha+\beta)^p \\ &= \sum_{i=0}^{p} \binom{p}{i} \alpha^i \beta^{p-i} \\ &= \binom{p}{p} \alpha^p + \binom{p}{0} \beta^p \\ &= \alpha^p + \beta^p \\ &= \varphi(\alpha) + \varphi(p),\end{aligned}$$

where the third equality holds as $p$ divides all the binomial coefficients $\binom{p}{i}$ for $1 \leq i \leq p-1$ (we showed this in a previous homework), and $p = 0$ in $R$. Multiplication is easier. □

**Lemma 3.** *Let $K$ be a <u>finite</u> field of characteristic $p$. Then every element of $K$ has a $p$-th root.*

*Proof.* We are trying to show that the Frobenius homomorphism is surjective. Since it is a map between finite sets of the same size, it suffices to show that it is injective. Since it is a homorphism, it suffices to show that it has zero kernel. To show this, suppose $\varphi(\alpha) = 0$. Then $\alpha^p = 0$. If $\alpha \neq 0$, then we may repeatedly multiply by $\alpha^{-1}$ on both sides to conclude that $1 = 0$, a contradiction. Thus, we must have that $\varphi$ is injective, as desired. □

By the above lemma, we have that the extension $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is separable. It is normal as $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$. Or alternately you can show that it is the splitting field of the minimal polynomial of a generator of the multiplicative group $\mathbb{F}_{p^n}^\times$.

□

(d) This extension is normal but not separable. For normality, consider the polynomial $g(y) = y^p - x^p \in \mathbb{F}_p(x^p)[y]$. Note that in $\mathbb{F}_p(x)[y]$ we have

$$(y - x)^p = y^p - x^p = g(y),$$

using lemma (2). So $\mathbb{F}_p(x)$ is the splitting field for $g$ over $\mathbb{F}_p(x^p)$, as $g$ splits there, and it is generated by the single root $x$.

To see that $\mathbb{F}_p(x^p) \subset \mathbb{F}_p(x)$ is not separable, let $h(y)$ be the minimal polynomial for $x$ over $\mathbb{F}_p(x^p)$. Since $g(x) = 0$, we have that $h(y)$ divides $g(y)$ in $\mathbb{F}_p(x^p)[y]$ (it turns out $h(y) = g(y)$, but we won't need to show this). Then in $\mathbb{F}_p(x)[y]$ we have

$$h(y) \mid g(y) = (y - x)^p$$

Furthermore, since $x \notin \mathbb{F}_p(x^p)$, we have that $h$ is of degree at least 2. Since $\mathbb{F}_p(x)[y]$ is a UFD, we have that $h(y) = (y - x)^n$ for some $n \geq 2$. But this shows that $h$ has a multiple root in $\mathbb{F}_p(x)$. Thus, we have demonstrated an irreducible polynomial in the base field with multiple roots in the extension field, so the extension is not separable, as desired.