Week 12 Final, Math B504 **Name:** *James Wang*
April 22, 2024

Problem 1:

We want to determine the splitting fields and their degree over $\mathbb{Q}$ for the following polynomials.

(a) $x^4 - 2$.

The roots of this polynomial are $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. Hence the splitting field of this polynomial must contain $\sqrt[4]{2}$ and i, which makes it $\mathbb{Q}(\sqrt[4]{2}, i)$. We can check that this field indeed contains and is generated by the 4 roots . We claim that $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$. This is because $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, and $\mathbb{Q}(i) \not\subseteq \mathbb{Q}(\sqrt[4]{2})$, because a set of $\mathbb{R}$ cannot contain a set of $\mathbb{C}$.

(b) $x^4 + 2$.

I do not know if there are smarter ways to do this. By observation, the roots of this polynomial are $\{e^{\pi i/4}\sqrt[4]{2}, e^{3\pi i/4}\sqrt[4]{2}, e^{5\pi i/4}\sqrt[4]{2}, e^{7\pi i/4}\sqrt[4]{2}\}$. More importantly, note that $\sqrt{2} = (\sqrt[4]{2})^4$ and $e^{\pi i/4} = \dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2}i$. so the splitting field of the given polynomial is again $\mathbb{Q}(\sqrt[4]{2}, i)$. By the previous part, we know $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$.

(c) $x^4 + x^2 + 1$.

Observe that this given polynomial is the result of the long division $(x^6 - 1)/(x^2 - 1)$, which means its roots are the 4 roots of $x^6 - 1$ that are not ± 1. Note that $x^6 - 1 = (x^3 - 1)(x^3 + 1)$, so the roots of the given polynomial are $\{\pm\zeta_3, \pm\zeta_3^2\}$, where $\zeta_3 = e^{2\pi i/3}$. Hence $\mathbb{Q}(\zeta_3)$ is the splitting field of the given polynomial. We know $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$, since we can factor $x^3 - 1 = (x - 1)(x^2 + x + 1)$, so the minimal polynomial of ζ_3 over $\mathbb{Q}$ is $x^2 + x + 1$, something of degree 2.

(d) $x^6 - 4$.

We see that this polynomial is reducible to $x^6 - 4 = (x^3 - 2)(x^3 + 2)$. The roots of this polynomial are therefore $\{\pm\sqrt[3]{2}, \pm\zeta_3\sqrt[3]{2}, \pm\zeta_3^2\sqrt[3]{2}\}$. Hence the splitting field of this polynomial must contain $\sqrt[3]{2}$ and $\zeta_3 = e^{2\pi i/3}$, which makes it $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. We can check that this field indeed contains and is generated by the 6 roots. We claim that $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$. This is because $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$. Since $\gcd(2, 3) = 1$, we know immediately that $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$.

Problem 2:

For any prime p and any nonzero $a \in \mathbb{F}_p$, we want to prove that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$. We use the hint to prove if γ is a root, then $\gamma + 1$ is also a root.

This is quick because recall that in a field of characteristic p, we have

$$(\gamma + 1)^p - (\gamma + 1) + a = \gamma^p + 1 - \gamma - 1 + a = \gamma^p - \gamma + a = 0,$$

given γ is a root. In fact, we can generalize this for any $\gamma + u$, where $u \in \mathbb{F}_p$, by Fermat's Little Theorem:

$$(\gamma + u)^p - (\gamma + u) + a = \gamma^p + u^p - \gamma - u + a = \gamma^p - \gamma + a + u^p - u = u^p - u = 0.$$

This tells us that the given polynomial has p distinct roots, which are $\gamma, \gamma + u_1, \ldots, \gamma + u_{p-1}$, where $u_1, \ldots, u_{p-1} \in \mathbb{F}_p$.

To prove irreducibility, we first observe that $\gamma \notin \mathbb{F}_p$, because otherwise we would have

$$0 = \gamma^p - \gamma + a = 0 + a,$$

thereby contradicting our initial assumption of $a \neq 0$. Now suppose for a contradiction that the given polynomial is reducible and factors into $x^p - x + a = f(x)p(x)$. Without loss of generality, suppose $\deg(f) = n < p$, then we know $f(x)$ is the product of n linear terms of the form $\{x - (\gamma + u_i)\}$, where each $(\gamma + u_i)$ is a root of the given polynomial. When we expand it, we know the coefficient of x^{n-1} will be $\sum(\gamma + u_i)$ by the Vieta Theorem. Also note that $f(x) \in \mathbb{F}_p[x]$, so $\sum(\gamma + u_i) \in \mathbb{F}_p$. We observe that the coefficient can be reduced to $n\gamma + \sum u_i$. Since each $u_i \in \mathbb{F}_p$, $\sum u_i \in \mathbb{F}_p$, so it must be that $n\gamma \in \mathbb{F}_p$. We claim that $n = 0$ in $\mathbb{F}_p$. Otherwise we can always multiply $n\gamma$ by the multiplicative inverse of n to get $\gamma \in \mathbb{F}_p$, which contradicts with our previous result of $\gamma \notin \mathbb{F}_p$. Hence we see that $n = 0$, which means $\deg(f) = 0$, thus showing the given polynomial $x^p - x + a$ is irreducible.

Finally, the part that $x^p - x + a$ is separable over $\mathbb{F}_p$ follows quickly from the fact that its p roots are all distinct.

$$QED$$

Problem 3:

Let σ_p be the Frobenius map $a \mapsto a^p$ on the finite field $\mathbb{F}_{p^n}$. We want to verify that σ_p is an automorphism of $\mathbb{F}_{p^n}$, and the order of σ_p is n.

We first show σ_p is a field homomorphism. Note that since $\mathbb{F}_{p^n}$ has characteristic p, we have $(a_1 + a_2)^p = a_1^p + a_2^p$:

$$\sigma_p(a_1 + a_2) = (a_1 + a_2)^p = a_1^p + a_2^p = \sigma_p(a_1) + \sigma_p(a_2),$$
$$\sigma_p(a_1 a_2) = (a_1 a_2)^p = a_1^p a_2^p = \sigma_p(a_1)\sigma_p(a_2).$$

Since σ_p is a nontrivial field homomorphism, it has to be injective, and since $\mathbb{F}_{p^n}$ is finite, it follows that σ_p is surjective. Hence σ_p is bijective, so it is indeed an automorphism of $\mathbb{F}_{p^n}$.

Since $\sigma_p^n(0) = 0$, we then show that applying the map n times to any nonzero element of $\mathbb{F}_{p^n}$ does not change the input, that $\sigma_p^n(a) = a$ for all $a \in \mathbb{F}_{p^n}^\times$. This follows from the fact that $\mathbb{F}_{p^n}^\times$ is a multiplicative group of order $p^n - 1$. Since the order of every element has to divide the order of the group, we have $a^{p^n-1} = 1$, so that $a^{p^n} = \sigma_p^n(a) = a$.

It remains to show n is the smallest integer such that $a^{p^n} = a$ for all $a \in \mathbb{F}_{p^n}^\times$. Suppose $m < n$, we want to show that $a^{p^m} \neq a$ for some $a \in \mathbb{F}_{p^n}^\times$. Recall that the multiplicative group of every finite field is cyclic, so there exists a generator $x \in \mathbb{F}_{p^n}^\times$ such that $x^k = a$ where $k \in \mathbb{Z}$ for all $a \in \mathbb{F}_{p^n}^\times$. Since x is the generator, it must be that $x^{p^n-1} = 1$ and $x^{p^n} = x$, and most importantly, $x^q \neq x$ for any $1 < q < p^n$. It follows quickly that $x^{p^m} \neq x$.

QED

Problem 4:

I read the proofs in the book. My main takeaway is that there is an algorithm to finding the roots and the splitting fields of polynomials of the form $x^n - k$, where k is a constant, but it is much more difficult to do so for polynomials with more terms. I found these results very useful when determining the degree of the splitting fields of polynomials in Problem 1.

For example, consider the polynomial $x^3 - 2$, and let $\zeta_3 = e^{2\pi i/3}$ be the primitive third root of unity. Then the roots of this polynomial are $\{\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}\}$, and the splitting field is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Since 1 is always a solution to $x^3 - 1$, we can factor $x^3 - 1 = (x-1)(x^2+x+1)$, so the minimal polynomial of ζ_3 over $\mathbb{Q}$ is $x^2 + x + 1$, something of degree 2. Since we also know that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, and $\gcd(2,3) = 1$, we can immediately conclude that $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$.

Generalizing this result a little, let $\zeta_n = e^{2\pi i/n}$ be the primitive nth root of unity. If n is prime, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = n - 1$. This is because $\phi(n) = n - 1$, and another way to see this is to consider the factorization $x^n - 1 = (x-1)(x^{n-1} + \cdots + 1)$ to see that 1 is already in the base field $\mathbb{Q}$ so the minimal polynomial of ζ_n is always of degree $n - 1$. We will later also see that the Galois group of this extension is always C_{n-1}.

One interesting example to consider is the roots of $x^4 - 1$, which are $\{\pm 1, \pm i\}$. Let $i = \zeta_4 = e^{2\pi i/4}$ be the primitive fourth root of unity. Since $\phi(4) = 2$, we know $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Another way to see this is that we have the factorization $x^4 - 1 = (x^2+1)(x^2-1)$, where ± 1 are the roots of $x^2 - 1$, so $x^2 + 1$ is the minimal polynomial of i, which is degree 2. In other words, only two of the four roots of unity are primitive: the new elements we get by adding in i.

Going back to our example, we can also see that $\zeta_3^{-2} = \zeta_3$, $\zeta_3^{-1} = \zeta_3^2$, $\zeta_3^3 = 1$, $\zeta_3^4 = \zeta_3$, $\zeta_3^5 = \zeta_3^2$, and so on so on.

Finally, let $\zeta_7 = e^{2\pi i/7}$ be the primitive seventh root of unity, it is also worth noting that in this example we have the linear dependence

$$\zeta_7^6 + \zeta_7^5 + \zeta_7^4 + \zeta_7^3 + \zeta_7^2 + \zeta_7 + 1 = 0,$$

which could be useful say if we are asked to compute the minimal polynomial of $\zeta_7 + \zeta_7^{-1}$.