Week 10 Final, Math B504 **Name:** *James Wang*
April 10, 2024

Problem 1:

We want to determine whether the following polynomials are irreducible in the rings indicated, and factor those that are reducible into irreducibles.

(a) $x^2 + x + 1$ in $\mathbb{F}_2[x]$.

Since this polynomial is a quadratic, if it were reducible, it has to be factored into two linear terms, meaning it has roots in $\mathbb{F}_2$. However, we see that in $\mathbb{F}_2$

$$0^2 + 0 + 1 = 1,$$
$$1^2 + 1 + 1 = 3 = 1,$$

which means neither of the two elements is a root for this polynomial. Hence it is irreducible.

(b) $x^3 + x + 1$ in $\mathbb{F}_3[x]$.

Since this polynomial is a cubic, if it were reducible, one of its factors has to be a linear term, meaning it has a root in $\mathbb{F}_3$. Indeed, we see that in $\mathbb{F}_3$

$$1^3 + 1 + 1 = 3 = 0,$$

so $(x - 1)$ is a factor of the given polynomial. We then divide the given polynomial with this term via long division, which gives

$$(x^2 + x + 1)/(x - 1) = x^2 + x + 2.$$

Since $x^2 + x + 2$ has no root in $\mathbb{F}_3$, we know it is irreducible in $\mathbb{F}_3$. We can then conclude that the factorization of the given polynomial into irreducibles is $(x - 1)(x^2 + x + 2)$.

(c) $x^4 + 1$ in $\mathbb{F}_5[x]$.

Since we are in $\mathbb{F}_5$, we know $x^4 + 1 = x^4 - 4$, which can be factored into quadratics

$$x^4 - 4 = (x^2 + 2)(x^2 - 2).$$

We can then easily see that neither of the two quadratic terms have roots in $\mathbb{F}_5$. Hence the factorization of the given polynomial into irreducibles is $(x^2 + 2)(x^2 - 2)$.

(d) $x^4 + 10x^2 + 1$ in $\mathbb{Z}[x]$.

Since this polynomial is a quartic, and it has no root by the Rational Root Theorem, we know if it were reducible, it has to be factored into two quadratics, such that

$$\begin{aligned} x^4 + 10x + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (c + a)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd, \end{aligned} \tag{1}$$

which means $bd = 1$, $ac + b + d = 0$, and $a + c = 0$. This system has no solution over $\mathbb{Z}$. Hence the given polynomial is irreducible.

(e) $x^4 - 4x^4 + 6$ in $\mathbb{Z}[x]$.

This polynomial is irreducible by the Eisenstein Criterion, by taking $p = 2$.

Problem 2:

We want to determine the degree of the following elements over $\mathbb{Q}$.

(a) $\alpha = 2+\sqrt{3}$.

Since $\alpha \in \mathbb{Q}(\sqrt{3})$, and $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, we know $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ has to divide 2. Clearly, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \neq 1$ because $\alpha \notin \mathbb{Q}$, so it must be $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

(b) $\alpha = 1+\sqrt[3]{2}+\sqrt[3]{4}$

We see that

$$\alpha^0 = 1$$

$$\alpha^1 = 1+\sqrt[3]{2}+\sqrt[3]{4}$$

$$\begin{aligned} \alpha^2 &= (1+\sqrt[3]{2}+\sqrt[3]{4})(1+\sqrt[3]{2}+\sqrt[3]{4}) \\ &= 1+\sqrt[3]{2}+\sqrt[3]{4}+\sqrt[3]{2}+\sqrt[3]{4}+2+\sqrt[3]{4}+2+2\sqrt[3]{2} \\ &= 5+4\sqrt[3]{2}+3\sqrt[3]{4} \end{aligned} \tag{2}$$

$$\begin{aligned} \alpha^3 &= (5+4\sqrt[3]{2}+3\sqrt[3]{4})(1+\sqrt[3]{2}+\sqrt[3]{4}) \\ &= 5+5\sqrt[3]{2}+5\sqrt[3]{4}+4\sqrt[3]{2}+4\sqrt[3]{4}+8+3\sqrt[3]{4}+6+\sqrt[3]{2} \\ &= 19+15\sqrt[3]{2}+12\sqrt[3]{4} \end{aligned} \tag{3}$$

This gives us a linear dependence, since $\alpha^3-3\alpha^2-3\alpha-1=0$. Hence the minimal polynomial for α over $\mathbb{Q}$ is x^3-3x^2-3x-1. Since the minimal polynomial is degree 3, we know $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Note: I know we can run a much more simple argument like what we did for part (a), but I wanted to do it this way to illustrate what I meant by we can always use this algorithm to compute the minimal polynomial during problem session.

(c) $\alpha = \sqrt{3 + 2\sqrt{2}}$.

By some arithmetic, we see that

$$\begin{aligned} \sqrt{3+2\sqrt{2}} &= \sqrt{2+2\sqrt{2}+1} \\ &= \sqrt{(\sqrt{2}+1)^2} \\ &= \sqrt{2}+1 \end{aligned} \tag{4}$$

Using similar logic to part (a), we can conclude that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

(d) $\alpha = \sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}}$.

We see that

$$\begin{aligned} \alpha^2 &= \left(\sqrt{1+\sqrt{-3}} + \sqrt{1-\sqrt{-3}}\right)^2 \\ &= 1 + \sqrt{-3} + 2\sqrt{(1+\sqrt{-3})(1-\sqrt{-3})} + 1 - \sqrt{-3} \\ &= 1 + \sqrt{-3} + 2\sqrt{4} + 1 - \sqrt{-3} \\ &= 6. \end{aligned} \tag{5}$$

This means $x^2 - 6$ is the minimal polynomial of α over $\mathbb{Q}$. Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

Problem 3:

Suppose $F = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$ for $i = 1, 2, \ldots, n$. We want to show that $\sqrt[3]{2} \notin F$.

Let $\alpha_i^2 = q \in \mathbb{Q}$, so that $\alpha_i^2 - q = 0$. We know there are two possibilities every time we add a new α_i into the field $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. The first case is that $\alpha_i^2 - q$ is reducible over the field $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, which means α_i is already in $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, so adding it does not produce a new field extension, and the degree of the extension does not change (multiplied by 1). The second case is that $\alpha_i^2 - q$ is irreducible over the field $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, which makes it a minimal polynomial of degree 2, so adding α_i produces a new field extension, and the degree of the extension is multiplied by 2. This means $[\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) : \mathbb{Q}] = 2^k$.

Now suppose for a contradiction that $\sqrt[3]{2} \in F$. We use the tower formula, because

$$[\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) : \mathbb{Q}] = [\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

Since we know $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, but $3 \nmid 2^k$, so we have reached a contradiction.

$$QED$$

Problem 4:

(a) We want to show that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

The inclusion $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ is obvious because a field has additive closure. We now show the other inclusion.

Since $\alpha = \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, we know the field $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ has to contain α^{-1}. We see that $(\sqrt{2}+\sqrt{3})(\sqrt{3}-\sqrt{2}) = 1$, so $\alpha^{-1} = \sqrt{3}-\sqrt{2}$. By the arithmetic closure of fields,

$$\frac{\alpha+\alpha^{-1}}{2} = \frac{2\sqrt{3}}{2} = \sqrt{3}$$
$$\frac{\alpha-\alpha^{-1}}{2} = \frac{2\sqrt{2}}{2} = \sqrt{2}$$

so we have $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Hence we get the other inclusion, and $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

QED

(b) We want to show that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$.

By our result from part (a), this is equivalent to showing $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$. Since by the Tower Formula $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$, and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, we just need to show that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

Since the minimal polynomial for $\sqrt{3}$ is x^2-3, which is degree 2, it suffices to show that x^2-3 is irreducible over $\mathbb{Q}(\sqrt{2})$. Suppose for a contradiction that this polynomial has a root in $\mathbb{Q}(\sqrt{2})$ such that $(a+b\sqrt{2})^2 = 3$, where $a,b \in \mathbb{Q}$. Then it must be that

$$a^2 + 2ab\sqrt{2} + 2b^3 = 3,$$

which implies $a^2+2b^2 = 3$ and $2ab = 0$. Since $\mathbb{Q}$ is an integral domain, the only solution to this system is $a = 0$ or $b = 0$. If $a = 0$, then we would have $2b^3 - 3 = 0$. If $b = 0$, then we would have $a^2 - 3 = 0$. In both cases, we can use the Eisenstein Criterion to conclude that the polynomials are irreducible. Hence they do not have roots in $\mathbb{Q}$. This means $a,b \notin \mathbb{Q}$, which is a contradiction.

QED

(c) We want to find the minimal polynomial of $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

Since we already know $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, we know $\{1, \alpha, \alpha^2, \alpha^3\}$ is a basis for $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$. This means if we raise α to α^4, we get a linear dependence. Indeed

$$\alpha^0 = 1$$

$$\alpha^1 = \sqrt{2} + \sqrt{3}$$

$$\alpha^2 = (\sqrt{2} + \sqrt{3})(\sqrt{2} + \sqrt{3}) = 2 + \sqrt{6} + \sqrt{6} + 3 = 5 + 2\sqrt{6}$$

$$\alpha^3 = (5 + 2\sqrt{6})(\sqrt{2} + \sqrt{3}) = 5\sqrt{2} + 5\sqrt{3} + 4\sqrt{3} + 6\sqrt{2} = 11\sqrt{2} + 9\sqrt{3}$$

$$\alpha^4 = (11\sqrt{2} + 9\sqrt{3})(\sqrt{2} + \sqrt{3}) = 22 + 11\sqrt{6} + 9\sqrt{6} + 27 = 49 + 20\sqrt{6}$$

and we see that $\alpha^4 + 10\alpha^2 + \alpha^0 = 0$, which means the minimal polynomial is $x^4 - 10x^2 + 1$.

$$QED$$