Math 404 HW 3 Solutions

1 Problem 3.1

Let $f \in k[x]$ be a degree n polynomial with roots $\alpha_1, \ldots, \alpha_n$. Define the discriminant as

$$\Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

(a) Show that Δ is a symmetric function

(b) If $f = x^3 + a_2 x + a_3$, express Δ in terms of the coefficients a_2, a_3.

1. Let $\sigma \in S_n$. Note that

$$\sigma \cdot \Delta = \prod_{i<j} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)})^2.$$

Thus, we wish to show

$$\prod_{i<j} (\alpha_i - \alpha_j)^2 = \prod_{i<j} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)})^2 \tag{1}$$

We look at these products term by term. Fix some $i < j$, so on the left hand side we have the term $f_{ij} = (\alpha_i - \alpha_j)^2$. Let $k, \ell = \sigma^{-1}(i), \sigma^{-1}(j)$. We know that $k \neq \ell$, so either $k < \ell$ or $k > \ell$.

If $k < \ell$ then on the right hand side we have the term

$$(\alpha_{\sigma(k)} - \alpha_{\sigma(\ell)})^2 = (\alpha_i - \alpha_j)^2 = f_{ij},$$

so the term f_{ij} on the left hand side of (1) also appears on the right hand side.

If $k > \ell$, then on the right hand side we have the term

$$(\alpha_{\sigma(\ell)} - \alpha_{\sigma(k)})^2 = (\alpha_j - \alpha_i)^2 = [(-1)(\alpha_i - \alpha_j)]^2 = f_{ij}$$

So the term f_{ij} also appears on the right hand side of (1). Thus, all the terms on the left hand side of (1) appear on the right hand side of (1). Replacing σ by σ^{-1} yields that all the terms on the right hand side of (1) appear on the left hand side of (1). Thus, both sides of (1) are products of the same terms arranged in a different order, and since multiplication is commutative, they are the same product.

(note, this reasoning also shows that if you define $\delta = \sqrt{\Delta}$, then $\sigma \cdot \delta = \pm\delta$, think about why this is the case. The positive or negative sign here is called the *sign* of the permutation σ)

□

2. Here we just give the formula, and leave the reasoning behind it to you. We have that

$$\boxed{\Delta = -4a_2^3 + 27a_3^3}$$

2 Problem 3.2

(a) Show that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ are linearly independent over $\mathbb{Q}$.

(b) Show that $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ are linearly independent over $\mathbb{Q}$

(a) Consider the field extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We will show that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and that $\{1, \sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$. First we show how the problem will follow from this. Assuming this claim has been proven, the argument of theorem 11.4 yields that $\{1 \cdot 1, 1 \cdot \sqrt{3}, \sqrt{2} \cdot 1, \sqrt{2} \cdot \sqrt{3}\}$ is a basis for for $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. But then the problem result follows from noting that $\sqrt{6} = \sqrt{2} \cdot \sqrt{3}$.

First, we prove the claim that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ has basis $\{1, \sqrt{2})$. Indeed, the polynomial $x^2 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein or the rational root test, so this claim follows from theorem 11.7.

Next we investigate the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$. This is a simple field extension with generator $\sqrt{3}$. This generator is a root of the polynomial $f = x^2 - 3$, which is irreducible over $\mathbb{Q}$ by the same argument as above, but it still remains to be seen if it is irreducible over the larger field $\mathbb{Q}(\sqrt{2})$. Once we show that f is irreducible over $\mathbb{Q}(\sqrt{2})$, then theorem 11.7 again will yield that $\{1, \sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$, as desired.

Since f is of degree two, it is irreducible if and only if it has no roots. To see that f has no roots in $\mathbb{Q}(\sqrt{2})$, suppose towards a contradiction that $\alpha = a + b\sqrt{2}$ is a root of f, with $a, b \in \mathbb{Q}$. Then we have

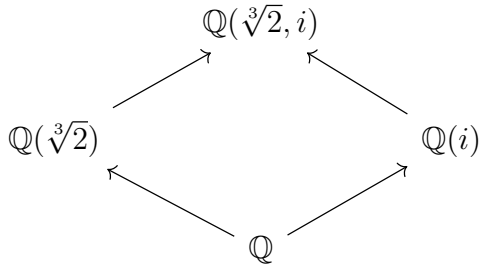
$$a^2 + 2b^2 + 2ab\sqrt{2} = 3$$

If neither a nor b are zero, then we get that $\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab}$, which yields that $\sqrt{2}$ is rational, which we proved false earlier in this problem. If $b = 0$, then we get $a^2 - 3 = 0$. But this is impossible, as $x^2 - 3$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion or the rational root test. If $a = 0$ then we get $2b^2 - 3 = 0$. But this is impossible, as $2x^2 - 3$ is

irreducible over $\mathbb{Q}$ by Eisenstein at 3 or the rational root test. This covers all possible values for a and b, so we must have that f has no roots, as desired.

□

(b) Suppose we have a linear dependence $a+b\sqrt[3]{2}+c\sqrt[3]{4}=0$, with $a,b,c \in \mathbb{Q}(i)$. We wish to show that $a=b=c=0$. Note that $\sqrt[3]{4}=(\sqrt[3]{2})^2$. Let $f=a+bx+cx^2 \in \mathbb{Q}(i)[x]$, so that $f(\sqrt[3]{2})=0$. If any of a,b, or c were nonzero, this would yield that the degree of the field extension $\mathbb{Q}(i)(\sqrt[2]{3})/\mathbb{Q}(i)$ was at most 2 (theorem 11.7 again). So it suffices to show that this extension has degree 3. This field extension naturally sits in the following diagram of field extensions

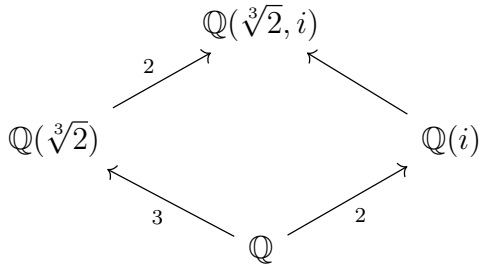


Now our goal is to figure out as many of the degrees in this picture as possible, and use the multiplicative property of the degree to figure out the rest.

The extensions $\mathbb{Q}(i)/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[2]{3},i)/\mathbb{Q}(\sqrt[2]{3})$ are each simple, generated by i. Note that i is a root of the polynomial $g=x^2+1$, which has no roots in $\mathbb{R}$. Since $\mathbb{Q} \subset \mathbb{R}$ and $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ (some real analysis shows that $\sqrt[3]{2}$ exists in $\mathbb{R}$), g has no roots in either of these fields, and so is irreducible over both of them. Thus, we have

$$[\mathbb{Q}(i):\mathbb{Q}]=[\mathbb{Q}(\sqrt[2]{3},i)/\mathbb{Q}(\sqrt[2]{3})]=2$$

The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has degree 3, as $\sqrt[3]{2}$ is a root of the polynomial x^3-2, which is irreducible over $\mathbb{Q}$ by Eisenstein or the rational root test. We repeat the preceding diagram, but with the known degrees of extension labeled.



Since the degree is multiplicative, using the left hand side of the above diagram, we get

$$[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[2]{3})] \cdot [\mathbb{Q}(\sqrt[2]{3}) : \mathbb{Q} = 6.$$

Using the other side of the above diagram, we get

$$6 = [\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(i)] \cdot 2$$

Thus, we get that $[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(i)] = 3$, as desired.

□

3 Problem 3.3

Let $f(x) \in F[x]$ be an irreducible degree n polynomial (so $n \geq 1$), with F a field. Then $\dim_F F[x]/(f) = n$.

Proof. We claim that the congruence classes $[1], [x], \ldots, [x^{n-1}]$ form a basis for $F[x]/(f)$.

Linear independence

Suppose that we have a linear dependence relation in $F[x]/(f)$

$$\begin{aligned} 0 &= b_0[1] + b_1[x] + \cdots + b_{n-1}[x^{n-1}] \\ &= [b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}] \end{aligned}$$

with $b_i \in F$. We wish to show that all $b_i = 0$. By definition of congruence classes, there exists some $g \in F[x]$ so that

$$fg = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1},$$

with the equality holding in $F[x]$. If $g \neq 0$, then we have that $\deg(fg) = \deg(f) + \deg(g) \geq \deg(f) = n$. However, looking at the right hand side of the above equation yields that $\deg(fg) \leq n - 1$, a contradiction. Thus, we must have that $g = 0$, so that

$$0 = fg = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$$

By definition of the polynomial ring, this means $b_i = 0$ for all i, as desired.

Spanning

. Let $\gamma \in F[x]/(f)$. Then we have that $\gamma = [g]$ for some $g \in F[x]$. Since f is nonzero, we may apply the division algorithm, and write

$$g = qf + r$$

with $\deg(r) < \deg(f) = n$. By definition of congruence classes, we have that

$$\gamma = [g] = [qf + r] = [r].$$

Furthermore, since $\deg(r) < n$, we uniquely write

$$r = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

with $c_i \in F$. Then we have that

$$\gamma = [r] = c_0 + c_1[x] + \cdots + c_{n-1}[x^{n-1}],$$

so that γ is in the span of $[1], \ldots, [x^{n-1}$, as desired. $\square$

Note, we didn't actually use irreducibility of f anywhere. Just that f was nonzero.

4 Problem 3.4

Eisenstein's criterion with a twist

(a) Let a be any integer. Let $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ is irreducible if and only if $f(x+a)$ is irreducible

(b) Use this trick to show that $x^3 - 3x^2 + 9x - 5$ is irreducible.

(c) Use this trick to show that, for any prime p, the polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible.

(a) First we show that $f(x+a)$ being irreducible implies $f(x)$ is irreducible. To do this, suppose we have a factorization $f(x) = g(x)h(x)$ with $f(x) \neq 0$. Define

$$\begin{aligned} f'(x) &:= f(x+a) \\ g'(x) &:= g(x+a) \\ h'(x) &:= h(x+a) \end{aligned}$$

So our assumption is that $f'(x)$ is irreducible, and we wish to show that exactly one of $g(x)$ or $h(x)$ is a unit. To do this, note that evaluating at $x+a$ is a homomorphism, so we have

$$f'(x) = g'(x)h'(x).$$

Since $f'(x)$ is irreducible, exactly one of $g'(x)$ or $h'(x)$ is a unit. Say without loss of generality that $g'(x)$ is a unit and $h'(x)$ is not.

Thus, there exists some polynomial $p'(x)$ so that $g'(x)p'(x) = 1$. Evaluating both sides of this equality at $x - a$ yields

$$1 = g'(x-a)p'(x-a) = g(x-a+a)p'(x-a) = g(x)p'(x-a).$$

Thus, $g(x)$ is a unit. So all that remains to be shown is that $h(x)$ is not a unit.

Suppose towards a contradiction that there is some polynomial $q(x)$ so that $h(x)q(x) = 1$. Then evaluating both sides at $x + a$ yields

$$1 = h(x + a)q(x + a) = h'(x)q(x + a),$$

contradicting our assumption that $h'(x)$ was a nonunit.

Thus, in any factorization $f(x) = g(x)h(x)$ exactly one of the two terms is a unit, and so f is irreducible, as desired.

Thus, we have shown that for any integer a, that if $f(x + a)$ is irreducible, then $f(x)$ is irreducible as well. For the reverse implication, suppose $f(x)$ is irreducible, and let $f'(x) = f(x + a)$. Then $f'(x + (-a)) = f(x)$, which is irreducible. Thus by the previous reasoning applied to the integer $-a$, we have that $f'(x)$ is irreducible, as desired.

□

Exercise *If you'll notice, all we used were that evaluating at $x+a$ and $x - a$ were inverse homomorphisms. So try and prove the following: Let $\varphi : R \xrightarrow{\sim} S$ be an isomorphism of integral domains. Then for any $r \in R$ we have that r is irreducible if and only if $\varphi(r)$ is irreducible.*

(b) Let $f(x) = x^3 - 3x^2 + 9x - 5$. Note that Eisenstein's criterion does not apply to f, but there are lots of evaluations of f after which Eisenstein's criterion applies. Here we write out the evaluations, and a prime for which Eisenstein's criterion applies

$$\begin{aligned} f(-1) &= -18 + 18x - 6x^2 + x^3 && (p = 2) \\ f(1) &= 2 + 6x + x^3 && (p = 2) \\ f(3) &= 22 + 18x + 6x^2 + x^3 && (p = 2) \end{aligned}$$

□

(c) Define

$$\begin{aligned} f(x) &= \sum_{i=0}^{p-1} x^i \\ g(x) &= x^p - 1, \end{aligned}$$

so that our goal is to show that $f(x)$ is irreducible. Note that

$$\begin{aligned} f(x) \cdot (x-1) &= \left(\sum_{i=0}^{p-1} x^i \right) \cdot (x-1) \\ &= \sum_{i=0}^{p-1} x^{i+1} - \sum_{i=0}^{p-1} x^i. \end{aligned}$$

All the terms in these two sums cancel out, except for the x^p and -1 terms, so that $f(x) \cdot (x-1) = x^p - 1$. Evaluating both sides at $x+1$ yields

$$f(x+1) \cdot x = (x+1)^p - 1 \tag{2}$$

By part (a) it suffices to show that $f(x+1)$ is irreducible. Expanding the right hand side of (2) using the binomial theorem yields

$$\begin{aligned} f(x+1) &= \frac{\left(\sum_{i=0}^{p} \binom{p}{i} x^i \right) - 1}{x} \\ &= \frac{\sum_{i=1}^{p} \binom{p}{i} x^i}{x} \\ &= \sum_{i=1}^{p} \binom{p}{i} x^{i-1}. \end{aligned}$$

We hope to apply Eisenstein's criterion to this polynomial. Indeed, the constant term of $f(x+1)$ gets a contribution when $i-1=0$, so $i=1$, with coefficient $\binom{p}{1} = p$, so p divides the constant term, and p^2 does not divide the constant term. The leading coefficient of $f(x+1)$ is $\binom{p}{p} = 1$, which is not divisible by p. So all that remains to be shown is that all the intermediate coefficients are divisible by p.

To do this, we expand the binomial coefficient for $2 \leq i \leq p-1$

$$\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-(i-1))}{i(i-1)(i-2)\ldots(2)\cdot 1} \tag{3}$$

(if you've seen a different formula for the binomial coefficients, check that it agrees with this one). If we're hoping that p divides this integer,

then we should be able to factor out the p in the numerator and write

$$\binom{p}{i} = p \cdot \frac{(p-1)(p-2)\cdots(p-(i-1))}{i(i-1)(i-2)\ldots(2)\cdot 1}. \tag{4}$$

The only problem that remains is how do we know that the fraction written here is actually an integer, and not just a rational number? The fraction in (3) is an integer because it is the answer to a combinatorial question, "How many i-element subsets of a set of size p are there?" (by the way, there's an orbit-stabilizer formula implicit in this formula, see if you can make sense of this)

To see that the fraction in (4) is an integer, we can imagine expanding all of the terms in each of the products for the numerator and denominator in (3) into their prime factorizations. Since the whole fraction is an integer, all the primes that appear as factors of the denominator must appear with potentially larger exponents in the numerator. However, since $i < p$ all of the prime factors in the denominator are also less than p, so they must appear with potentially larger exponents in the terms $p - j$ for $j \geq 1$ in the numerator. They can't appear in the p term in the numerator. That is, all the factors denominator in (4) cancel with some of the factors in the numerator in (4). That is, the fraction in (4) is an integer, as desired.

5 Problem 3.5

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

(b) Find a single generator for $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

(a) We will prove that $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$ in a few different ways.

5.1 Direct Computation

Consider the field extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. The first extension has degree 2 as $x^2 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein or the rational root test.

The multiplicative property of the degree shows that it suffices to prove that the extension $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ is of degree 3. Note that this extension is generated by an element which is a root of the polynomial $f = x^3 - 2$. If f is irreducible over $\mathbb{Q}(\sqrt{2})$, then the extension will be degree 3. Since f is of degree 3, it suffices to show that f has no roots in $\mathbb{Q}(\sqrt{2})$.

So suppose towards a contradiction that $\alpha^3 - 2 = 0$, for some $\alpha \in \mathbb{Q}(\sqrt{2})$ We've shown earlier in this homework that $1, \sqrt{2}$ forms a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, so we may uniquely write $\alpha = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$. Then we compute

$$0 = (a + b\sqrt{2})^3 - 2 = a^3 + 2b^3\sqrt{2} + 3a^2b\sqrt{2} + 6ab^2 - 2$$

Rearranging this equation yields

$$\sqrt{2}(2b^3 + 3a^2b) + a^3 + 6ab^2 - 2 = 0$$

Since 1 and $\sqrt{2}$ are linearly independent over $\mathbb{Q}$, this is equivalent to the pair of equations

$$\begin{aligned} b(2b^2 + 3a^2) &= 0 \\ a^3 + 6ab^2 - 2 &= 0 \end{aligned}$$

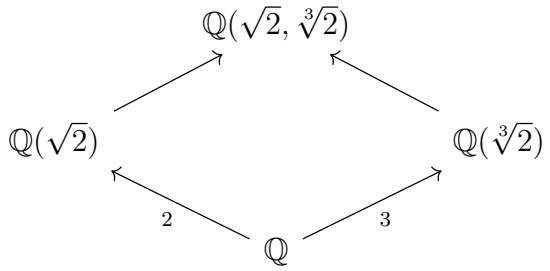
The first equation yields that either $b = 0$ or $2b^2 + 3a^2 = 0$. However, since $a, b \in \mathbb{R}$ we have $2b^2 + 3a^2 \geq a^2 + b^2 \geq 0$, with the second holding if and only if $a = b = 0$. However if $a = b = 0$ then the second equation above does not hold. Thus, we can not have $2b^2 + 3a^2 = 0$, so we must have $b = 0$.

But then the second equation above reads $a^3 - 2 = 0$, which is impossible as $a \in \mathbb{Q}$ and $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein or the rational root test. Thus, our pair of equations can not be solved, and the result holds.

□

5.2 Leveraging the multiplicative property of the degree

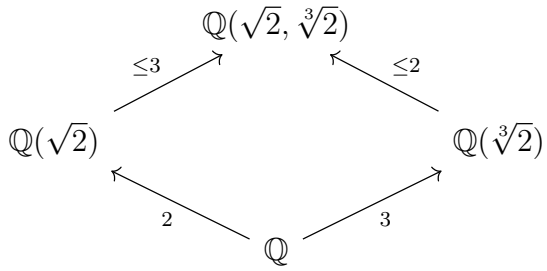
Consider the diagram of field extensions, with easy to compute degrees labeled.



Let f be the minimal polynomial for $\sqrt[3]{2}$ over $\mathbb{Q}(\sqrt{2})$. Since $\sqrt[3]{2}$ is a root of $g = x^3 - 2 \in \mathbb{Q}(\sqrt{2})[x]$, we have that f divides g. Thus, we have that

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] = \deg f \leq \deg g = 3.$$

Similar reasoning yields that we can fill out this diagram with degree inequalities



Using the multiplicative property of the degree, we have that

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \leq 3 \cdot 2 = 6.$$

So the overall degree is at most 6. But using the multiplicative property of the degree moving along each side of the above diagram yields that 2 and 3 each divide $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$. Thus, we have that the least common multiple of 2 and 3 divides $[[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$. That is, we have that 6 divides $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$, so we have

$$6 \leq [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] \leq 6,$$

so we must have equality throughout.

□

Exercise This same reasoning works in greater generality. Suppose we have a field k and elements α, β each algebraic over k with $n = [k(\alpha) : k]$ and $m = [k(\beta) : k]$ relatively prime. Compute $[k(\alpha, \beta) : k]$

5.3 Finding a single generator

Use some of the early ideas in the preceding parts to show that

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] \leq 6.$$

For the reverse inequality it suffices to give an element $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ of degree 6 over $\mathbb{Q}$, as then $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ yields

$$6 \geq [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 6,$$

so we must have equality throughout. This would also show that $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\alpha)] = 1$, so that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\alpha)$, solving (b) along the way. So all that remains is to find an α of degree 6 over $\mathbb{Q}$, which we do in part (b)

□

(b) From part (a), we are in search of some element $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ of degree 6 over $\mathbb{Q}$. To find one, note that

$$\left(\frac{\sqrt{2}}{\sqrt[3]{2}}\right)^6 = \frac{2^3}{2^2} = 2.$$

Thus, if we let $\alpha = \frac{\sqrt{2}}{\sqrt[3]{2}}$, we have that $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ and α is a root of $f = x^6 - 2 \in \mathbb{Q}[x]$. Note that f is irreducible by Eisenstein at the prime 2 (rational root test isn't enough here), so α is of degree 6, as desired.