SOME PROPERTIES OF EXTENSIONS OF SMALL DEGREE OVER $\mathbb{Q}$

TREVOR ARNOLD

Abstract. This paper demonstrates a few characteristics of finite extensions of small degree over the rational numbers $\mathbb{Q}$. It comprises attempts at classification of all such extensions of degrees 2, 3, and 4, as well as mention of how one might begin the process of classifying all finite fields with degree a power of 2. Some topics discussed are discriminants of certain fields, how to represent a given extension as a simple extension, and some applied Galois theory.

1. Quadratic Extensions

It is fairly clear why quadratic extensions are in most respects the easiest to understand: they all have the same Galois group ($\mathbb{Z}_2$), their degree over $\mathbb{Q}$ is as small as possible without being trivial, and the number 2 is in many ways very easy to work with.

1.1. **The Make-up of a Quadratic Number Ring.** We begin by completely classifying the elements of the number ring associated with any number field of the form $\mathbb{Q}(\sqrt{m})$, where $m \neq 1$ or 0, is squarefree (i.e. a *quadratic number field*). This ring is by definition simply $\mathbb{A} \cap \mathbb{Q}(\sqrt{m})$, where $\mathbb{A}$ is the set of *algebraic integers*, defined here to be the set

$$\{\alpha \in \mathbb{C} : \exists\ f(x) \in \mathbb{Z}[x] \ni f(\alpha) = 0, f(x) \text{ monic and irreducible}\}.$$

1.1.1. *Preliminaries.* We know that $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$, and so any element of $\mathbb{A} \cap \mathbb{Q}(\sqrt{m})$ is going to have a minimum polynomial $f(x)$ with $\deg f(x) \leq 2$. Thus we know that the algebraic numbers in $\mathbb{Q}(\sqrt{m})$ will simply be those elements $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$ for some $f(x) \in \mathbb{Z}$, monic and irreducible, with $\deg f(x) \leq 2$. Our goal in section **??** will be to show that any root of such a polynomial can be expressed in one of the following ways:

- as $a + b\sqrt{m}$, where $a, b \in \mathbb{Z}$ and $m \equiv 2$ or $3 \pmod 4$, for some squarefree m
- or as $\frac{a+b\sqrt{m}}{2}$, where $a, b \in \mathbb{Z}$, $a \equiv b \pmod 4$, and $m \equiv 1 \pmod 4$, for some squarefree m.

Date: May 15, 2000.

This is trivial to show if $\deg f(x) < 2$, and so we will only give a treatment of the case where f is a genuine quadratic.

1.1.2. *Roots of quadratic polynomials.* Take any $f(x) = x^2 + cx + d \in \mathbb{Z}[x]$. By an elementary theorem of arithmetic, we know that

$$f(x) = 0 \;\Leftrightarrow\; x = \frac{-c \pm \sqrt{c^2 - 4d}}{2}.$$

Choosing t and m appropriately, we can write $c^2 - 4d = t^2 m$ where m is squarefree. Since $t \equiv 0$, 1, 2, or 3 $\pmod 4$, it follows that $t^2 \equiv 0$ or 1 $\pmod 4$. This gives us two cases.

If $t^2 \equiv 0 \pmod 4$, we have

$$4|c^2 - 4d \;\Rightarrow\; 4|c^2 \;\Rightarrow\; 2|c \;\Rightarrow\; \frac{-c}{2} \pm \frac{t}{2}\sqrt{m} \in \mathbb{Z},$$

and hence we know that any root of $f(x)$ has the form $a + b\sqrt{m}$, $a, b \in \mathbb{Z}$. This is what we want for $m \equiv 2$ or 3 $\pmod 4$, and for $m \equiv 1 \pmod 4$, we simply note that

$$a + b\sqrt{m} = \frac{2a + 2b\sqrt{m}}{2} \text{ where } 0 \equiv 2a \equiv 2b \pmod 2.$$

If $t^2 \equiv 1 \pmod 4$, consider the possibility that $m \equiv 2$ or 3 $\pmod 4$. We would have

$$c^2 - 4d \equiv c^2 \equiv 1 \cdot 2 \text{ or } 1 \cdot 3 \equiv 2 \text{ or } 3 \pmod 4,$$

which is an impossibility for the square of an integer (see above). Thus we must have $m \equiv 1 \pmod 4$ since m is assumed to be squarefree, and therefore

$$c^2 - 4d \equiv c^2 \equiv t^2 m \equiv 1 \cdot 1 \equiv 1 \pmod 4.$$

Hence t and c are both odd (or else $t^2 \equiv c^2 \equiv 0 \pmod 4$). From all of this it follows that when $t^2 \equiv 1 \pmod 4$, $-c \equiv \pm t \pmod 2$ and $m \equiv 1 \pmod 4$.

Thus we have shown explicitly that all roots of a monic quadratic polynomial $f(x) \in \mathbb{Z}[x]$ have the form stated above, from which it directly follows that any $\alpha \in \mathbb{A} \cap \mathbb{Q}(\sqrt{m})$ also has this form for some m.

1.2. **The Discriminant.** Now that we have shown what an element of $\mathbb{A} \cap \mathbb{Q}(\sqrt{m})$ has to look like, we want to know if everything of this form has to be in $\mathbb{A} \cap \mathbb{Q}(\sqrt{m})$ for some m; more specifically, we want to show

$$\mathbb{A} \cap \mathbb{Q}(\sqrt{m}) = \begin{cases} \{a + b\sqrt{m}\} & m \equiv 2 \text{ or } 3 \pmod 4 \\ \left\{ \frac{a+b\sqrt{m}}{2} : a \equiv b \pmod 2 \right\} & m \equiv 1 \pmod 4 \end{cases}.$$

Once we know this, it will be clear that the following will be a set of generators for $\mathbb{A} \cap \mathbb{Q}(\sqrt{m})$ as a $\mathbb{Z}$-module (i.e. an *integral basis*):

$$\begin{cases} \left\{1, \sqrt{m}\right\} & \text{when } m \equiv 2 \text{ or } 3 \pmod 4, \\ \left\{1, \dfrac{1+1\sqrt{m}}{2}\right\} & \text{when } m \equiv 1 \pmod 4. \end{cases}$$

From this we will be able to directly compute the discriminant of $\mathbb{Q}(\sqrt{m})$.

1.2.1. *Preliminaries.* Although we have shown explicitly what the elements of a number field look like, we have as yet to show that if $\frac{a+b\sqrt{m_1}}{2} \in \mathbb{A} \cap \mathbb{Q}(\sqrt{m_2})$ then necessarily $m_1 = m_2$. We do this here in preparation for demonstrating that the generators are exactly what we want them to be. It is clear that the result will follow immediately if we can show

$$\mathbb{Q}(\sqrt{m_1}) \cap \mathbb{Q}(\sqrt{m_2}) = \mathbb{Q},$$

so this how we shall proceed.

From elementary field theory, we want to show that one of the two conditions

- $\mathbb{Q}(\sqrt{m_1}) \cap \mathbb{Q}(\sqrt{m_2}) = \mathbb{Q}$
- $\mathbb{Q}(\sqrt{m_1}) = \mathbb{Q}(\sqrt{m_2})$

must hold, which we will be able to conclude from the following:

- $\left[\mathbb{Q}(\sqrt{m_1}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\sqrt{m_2}) : \mathbb{Q}\right] = 2$
- both $\mathbb{Q}(\sqrt{m_1})$ and $\mathbb{Q}(\sqrt{m_2})$ contain $\mathbb{Q}(\sqrt{m_1}) \cap \mathbb{Q}(\sqrt{m_2})$
- $\left[\mathbb{Q}(\sqrt{m_1}) \cap \mathbb{Q}(\sqrt{m_2}) : \mathbb{Q}\right] = 1$ or 2.

Thus all that we will need to show is that if there is some $\beta \notin \mathbb{Q}$ with $\beta \in \mathbb{Q}(\sqrt{m_1}) \cap \mathbb{Q}(\sqrt{m_2})$, then it must be the case that $m_1 = m_2$.

There will be such a $\beta = a_1 + b_1\sqrt{m_1} = a_2 + b_2\sqrt{m_2}$ with $a_i, b_i \in \mathbb{Q}$ if and only if we can find rational numbers a and b such that $a + b\sqrt{m_1} = \sqrt{m_2}$. But then we would have the following:

$$m_2 = a^2 + 2ab\sqrt{m_1} + b^2 m_2 \in \mathbb{Z} \;\Rightarrow\; a = 0 \text{ or } b = 0.$$

If $a = 0$ then $m_2 = b^2 m_1$. Say $b = \frac{c}{d}$ (where $c, d \in \mathbb{Z}$ are relatively prime, $c \neq 0$, and $d \neq 0$). We then have $d^2 m_2 = c^2 m_1$. First off, we may assume that $c \neq 1$, because if so, we would either have m_1 not squarefree (in the case that $d \neq 1$), or we would have $m_1 = m_2$ (if $d = 1$), which we assumed wasn't the case. But since $(c, d) = 1$, we know that $(c^2, d^2) = 1$, and hence that for any p^2 dividing c^2, it is also the case that $p^2 | m_2$, contradicting the assumption that m_2 is squarefree. On the other hand, if $b = 0$, then $m_2 = a^2$, again contradicting the fact that m_2 is

squarefree (since we know in this case that a^2, and hence a, is necessarily in $\mathbb{Z}$ since $a \in \mathbb{Q}$). Thus we know there can be no such β, and hence $\mathbb{Q}(\sqrt{m_1}) \cap \mathbb{Q}(\sqrt{m_2}) = \mathbb{Q}$.

1.2.2. *A complete description of* $\mathbb{A} \cap \mathbb{Q}(\sqrt{m})$. What we have shown so far (combining sections **??** and **??**) is that

$$\mathbb{A} \cap \mathbb{Q}(\sqrt{m}) \subseteq \begin{cases} \{a + b\sqrt{m}\} & m \equiv 2 \text{ or } 3 \pmod 4 \\ \left\{ \frac{a+b\sqrt{m}}{2} : a \equiv b \pmod 2 \right\} & m \equiv 1 \pmod 4 \end{cases}.$$

What we want to show now is '$\supseteq$', which will prove to be relatively straightforward. Once we have done this, all that we need to do to find the discriminant will be a short, simple calculation.

Let $\frac{a+b\sqrt{m}}{2}$ be in one of the sets on the right hand side of the above equation (where $a \equiv b \pmod 2$ and where a and b are odd only if $m \equiv 1 \pmod 4$). This is clearly a root of the following polynomial:

$$x^2 - ax + \frac{a^2 - b^2 m}{4}.$$

Thus all we need to show is that $\frac{a^2-b^2m}{4} \in \mathbb{Z}$. We consider two cases. If a and b are even then $4|a^2$ and $4|b^2$ so $4|a^2 - b^2m$. If a and b are odd, then (by assumption) $m \equiv 1 \pmod 4$. Since a and b are odd, we have

$$\begin{aligned} a^2 \equiv b^2 \equiv 1 \pmod 4 &\Rightarrow a^2 - b^2 m \equiv 1 - 1 \cdot 1 \equiv 0 \pmod 4 \\ &\Rightarrow 4|a^2 - b^2 m \Rightarrow x^2 - ax + \frac{a^2 - b^2}{2} \in \mathbb{Z}[x]. \end{aligned}$$

We can therefore conclude that $\mathbb{A} \cap \mathbb{Q}(\sqrt{m})$ is in fact equal to what we want it to be.

1.2.3. *The discriminant: summing up.* Now that we have our hands on exactly what the makeup of a quadratic number ring is, we can take the integral basis that we have found and plug them into the defining formula for the discriminant. For $m \equiv 2 \text{ or } 3 \pmod 4$, we know that $\{1, \sqrt{m}\}$ is an integral basis, and that the only conjugate of $\sqrt{m}$ is $-\sqrt{m}$. Hence:

$$\mathit{disc}\left(\mathbb{Q}(\sqrt{m})\right) = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = \left(-\sqrt{m} - \sqrt{m}\right)^2 = \left(-2\sqrt{m}\right)^2 = 4m.$$

For $m \equiv 1 \pmod 4$, a set of generators over $\mathbb{Z}$ is $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$; the conjugate of $\frac{1+\sqrt{m}}{2}$ is $\frac{1-\sqrt{m}}{2}$. Hence:

$$\mathit{disc}\left(\mathbb{Q}(\sqrt{m})\right) = \begin{vmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{vmatrix}^2 = \left(\frac{1-\sqrt{m}}{2} - \frac{1+\sqrt{m}}{2}\right)^2 = \left(-\sqrt{m}\right)^2 = m.$$

And so we have established the following formulae for the discriminant of any quadratic number field:

$$disc\left(\mathbb{Q}(\sqrt{m})\right) = \begin{cases} 4m & \text{if } m \equiv 2 \text{ or } 3 \pmod 4 \\ m & \text{if } m \equiv 1 \pmod 4 \end{cases}$$

2. Degree 3 Extensions

Degree 3 extensions are nearly as routine as those of degree 2, and for many of the same reasons, e.g. their Galois groups are always isomorphic to $\mathbb{Z}_3$. In this section, we will show which cubic polynomials have splitting fields of degree 3 over $\mathbb{Q}$ and what the discriminant of a simple radical extension of degree 3 over $\mathbb{Q}$ is, following the outline on pp. 45–50 of [**?**] (and Ex. 41 in particular).

2.1. **Cubic Polynomials.** In this section, it will be necessary to introduce the concept of the discriminant of a polynomial. Say $f(x) \in F[x]$, F a field, has roots $x_1, \ldots, x_n$ in its splitting field $K \supseteq F$. The *discriminant* D_f of f is defined by the formula

$$D = D_f = \prod_{1 \le i < j \le n} (x_i - x_j)^2.$$

It is clear that for any $\phi \in G(K : F)$, which acts by necessity as a permutation on the roots, then $\phi(D) = D$. Since D is fixed by every element of the Galois group, it must be the case that $D \in F$.

We proceed to find necessary and sufficient conditions for a cubic polynomial to have a splitting field of degree 3 over $\mathbb{Q}$ (as outlined on p. 123 of [**?**]). Assume that $f(x) \in \mathbb{Q}[x]$ is monic and irreducible of degree 3, say

$$f(x) = x^3 + ax^2 + bx + c.$$

It can be shown by lengthy and tedious calculation (or the command

```
[> discrim(x^3 + a*x^2 + b*x + c, x);
```

in Maple) that in fact $D_f = -27c^2 + 18cab + a^2b^2 - 4a^3c - 4b^3$. It will be convenient to define the value d to be a square root of D, i.e.

$$d = \pm \prod_{1 \le i < j \le n} (x_i - x_j),$$

where we may choose the sign arbitrarily. It is clear that $d \in K$, the splitting field for f over $\mathbb{Q}$. Also convenient will be the variable change $x \mapsto u - a/3$, which yields

$$f(x) = g(u) = u^3 + pu + q$$

for some $p, q \in \mathbb{Q}$. We note that $D_g = D_f$ since our variable change simply translates the roots of f, and hence, for our purposes, we may assume that $a = 0$ to

begin with. Thus we have $D_f = -27c^2 - 4a^3c$. The Galois group G of K over $\mathbb{Q}$ can be viewed as a subgroup of S_3, the symmetric group on 3 letters, acting on the three roots of f (which must be distinct since f is irreducible, and hence separable, over $\mathbb{Q}$). Furthermore, G must act transitively on the roots of f. The only transitive subgroups of S_3 are S_3 itself and $A_3 \cong \mathbb{Z}_3$, the alternating subgroup comprising all even permutations of S_3. It is clear that if $\phi \in \mathbb{Q}$ is even, then $\phi(d) = d$ (indeed, this is one way to define the term "even"), i.e. $G \cong A_3 \cong \mathbb{Z}_3$ if and only if $\phi(d) = d$ for each $\phi \in G$, i.e. if and only if $d \in \mathbb{Q}$. Since the Fundamental Theorem of Galois Theory tells us that the degree of a Galois extension is equal to the order of its Galois group, we have shown that $[K : \mathbb{Q}] = 3$ if and only if $d \in \mathbb{Q}$, i.e. D is a square in $\mathbb{Q}$.

2.2. **Discriminants.** Following the sketch in [**?**], we will now show how to find the discriminant of $\mathbb{Q}(\sqrt[3]{m})$ where m is a cubefree integer. We will need to use a standard theorem from algebraic number theory (taken from [**?**]), stated here without proof:

Theorem *If R is a number ring and $\alpha \in R$ has degree n over $\mathbb{Q}$, then there is a basis for R over $\mathbb{Z}$ of the form*

$$1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}$$

where $d_i \in \mathbb{Z}$ with $d_1 \mid d_2 \mid \cdots \mid d_{n-1}$ and $f_i \in \mathbb{Z}[x]$ is monic and of degree i.

The idea, of course, is to use this to find an integral basis for $\mathbb{Q}(\sqrt[3]{m})$ in this form, after doing which it will be a straightforward calculation to find the discriminant of this field. We begin by verifying some needed facts.

2.2.1. *A few preparations.* Let K be an extension of $\mathbb{Q}$ of degree n and choose any two subsets of K $\{\eta_1, \ldots, \eta_n\}$ and $\{\theta_1, \ldots, \theta_n\}$ which generate the same $\mathbb{Z}$-submodule. Then there is a matrix M over $\mathbb{Z}$ such that

$$\begin{bmatrix} \eta_1 \\ \vdots \\ \eta_n \end{bmatrix} = M \begin{bmatrix} \theta_1 \\ \vdots \\ \theta_n \end{bmatrix}.$$

If $\sigma_1, \ldots, \sigma_n$ are the n isomorphisms between K and other subfields of $\mathbb{C}$, then we may apply each σ_i to the system of equations above to yield the matrix equation

$$\big[\sigma_j(\eta_i)\big] = M\big[\sigma_j(\theta_i)\big],$$

which yields, according to the definition of the discriminant of an n-tuple,

$$\mathit{disc}\,(\eta_1, \ldots, \eta_n) = |M|^2\, \mathit{disc}\,(\theta_1, \ldots, \theta_n)\,.$$

Since the determinant of M must be an integer, we may conclude that in fact

$$disc\,(\eta_1, \ldots, \eta_n) \leq disc\,(\theta_1, \ldots, \theta_n)\,.$$

Equality follows from the fact that our argument is symmetric.

It is an easy application of this result that

$$disc\,(\alpha) = \mathrm{disc}\big(1, f_1(\alpha), \ldots, f_{n-1}(\alpha)\big)$$

for $\alpha \in R$ =and it follows from the definition of the discriminant that

$$(*) \qquad disc\,(\alpha) = (d_1 d_2 \ldots d_{n-1})^2 disc\,\big(\mathbb{Q}(\sqrt[3]{m})\big)$$

since $1, f_1(\alpha), \ldots, f_{n-1}(\alpha)$ is an integral basis for $\mathbb{Q}(\sqrt[3]{m})$. Now choose two positive integers i and j such that $i + j < n$. Then we know that $f_i(\alpha) f_j(\alpha)$ is monic of degree $i + j$ and hence

$$\frac{f_i(\alpha) f_j(\alpha)}{d_i d_j} = \frac{d_{i+j} + \sum_{k=1}^{i+j} m_k d_1 \ldots d_k f_k(\alpha)}{d_{i+j}} \quad m_k \in \mathbb{Z},$$

implying that $d_i d_j \mid d_{i+j}$. Inductively then we can see that for $i < n$, $d_1^i \mid d_i$, and hence by (**??**), we have that $d_1^{n(n-1)} \mid disc\,(\alpha)$.

2.2.2. *An integral basis.* The general manner in which we will proceed to find our integral basis for $\mathbb{Q}(\sqrt[3]{m})$ is by considering and rejecting various possibilities. In order to keep notation consistent with the preceding section, we set $K = \mathbb{Q}(\sqrt[3]{m})$ and $\alpha = \sqrt[3]{m}$. Furthermore, we choose two relatively prime, squarefree integers h and k such that $m = hk^2$. To start things off, we will show that $disc\,(\alpha) = -27m^2$. To do this, we use the formula for the discriminant given by

$$disc\,(\alpha) = \pm \mathrm{N}_{K/\mathbb{Q}}\big(m'_{\alpha,\mathbb{Q}}(\alpha)\big),$$

where $m_{\alpha,\mathbb{Q}}(x)$ is the minimum polynomial for α over $\mathbb{Q}$ and "+" holds if and only if $n \equiv 0$ or $1 \pmod 4$. Since $m_{\alpha,\mathbb{Q}}(x) = x^3 - m$,

$$disc\,(\alpha) = -\mathrm{N}_{K/\mathbb{Q}}(3\alpha^2) = -3\alpha^2 \cdot 3\zeta\alpha^2 \cdot 3\zeta^2\alpha^2 = -27m^2,$$

where ζ is a primitive 3^{rd} root of unity. Thus, by the fact that $d_1^6 \mid disc\,(\alpha) = -27m^2$, we know that $d_1 = 1$ or 3, and can only equal 3 when $9 \mid m$. However, if $9 \mid m$ we have $\beta = (\alpha + a)/3 \in R$ for some integer a. But then $\mathrm{Tr}(\beta^3) \in \mathbb{Z}$, and

$$\mathrm{Tr}(\beta^3) = \mathrm{Tr}\left(\frac{1}{27}m + \frac{1}{9}a\alpha^2 + \frac{1}{9}a^2\alpha + \frac{1}{27}a^3\right) = \frac{m + a^3}{9} \in \mathbb{Z}$$

implies that $3 \mid a$ (since $9 \mid m$), which is impossible since then $\alpha/3 \in R$ and hence $m/27 \in R$, contradicting the fact that m is cubefree (the only rational numbers in a number ring are integers). Thus we have shown that $d_1 = 1$ in any case, and hence we may choose $f_1(\alpha) = \alpha$.

Now we attack f_2 and d_2. We will need the fact that $\alpha^2/k \in R$, which is shown simply by the fact that it is a root of $x^3 - h^2k$. Now let $m \equiv \pm 1 \pmod 9$ and let $\beta = (\alpha \mp 1)^2/3$. It is easy to compute that

$$\beta^3 - \beta^2 + \frac{1 \pm 2m}{3}\beta - \frac{(m \mp 1)^2}{27} = 0,$$

which tells us that $\beta \in R$ (which follows from our assumption that $m \equiv \pm 9 \pmod 9$), and so too is $\alpha\beta/3 = (\alpha^2 \pm k^2\alpha + k^2)/3k$. Note that this implies that when $m \equiv \pm 1 \pmod 9$, $3k \mid d_2$ (we have shown before that $k \mid d_2$ when $m \not\equiv \pm 1 \pmod 9$). By the previous section, we know that $d_2^2 \mid disc\,(\alpha) = -27m^2$, implying that $d_2 \mid 3m$. In order to work with the coefficients of f_2, it will be convenient to say $f_2(\alpha) = \alpha^2 + a\alpha + b$ for some integers a and b.

In order to start determining which primes can divide d_2, we now choose a prime number p such that $p \neq 3$, $p \mid m$, and $p^2 \nmid m$. If $p \mid d_2$ then it is clear that $(\alpha^2 + a\alpha + b)/p \in R$. Taking the trace of this yields

$$\mathrm{Tr}\left(\frac{\alpha^2 + a\alpha + b}{p}\right) = \frac{3b}{p} \in \mathbb{Z},$$

and hence $p \mid b$, implying that $(\alpha^2 + a\alpha) \in R$. But then cubing this yields

$$\mathrm{Tr}\left(\frac{m^2 + 3m\alpha^2 + 3a^2\alpha + a^3m}{p^3}\right) = \frac{3(m^2 + a^3m)}{p^3} \in \mathbb{Z},$$

and hence $p^3 \mid m(m + a^3)$, implying that $p^2 \mid m + a^3$ (since $p \mid m$). But then (again since $p \mid m$) $p \mid a^3$, and it follows that $p^2 \mid a^3$ and hence $p^2 \mid m$, a contradiction. Thus no such prime can divide d_2. So suppose $p \neq 3$ and $p^2 \mid m$. We know from above that $k \mid d_2$. Since $p^2 \mid m$, it must be that $p \mid k$, and hence $p \mid d_2$. If $p^2 \mid d_2$, by the same reasoning as above we obtain $p^6 \mid m(m + a^3)$ and hence $p^3 \mid m$, another contradiction. Thus $p^2 \nmid d_2$ for such primes. At this point we know that $d_2 = 3^i k$ for some i. If we square $f_2(\alpha)/d_2$, we get the following:

$$\frac{m\alpha + 2a^2m + a^2\alpha^2 + 2ab\alpha + b^2}{d_2^2} \in R,$$

which implies that d_2 divides all of $a^2 + 2b$, $m + 2ab$, and $b^2 + 2am$, since no ratio in R can have a denominator greater than d_2.

To find the power of 3 dividing d_2, first consider the case where $3 \nmid m$. We have already shown that $d_2 \mid 3m$, and so it is easy to conclude that $9 \nmid d_2$. When $m \equiv \pm 1 \pmod 9$, we already know that d_2 is divisible by 3 since it is divisible by $3k$. If $m \not\equiv \pm 1 \pmod 9$, suppose $3 \mid d_2$. If a or $b \equiv 0 \pmod 3$, then $m \equiv 0 \pmod 3$ since 3 divides $m + 2ab$. However, we know that $a^2 + 2b \equiv 0 \pmod 3$ and so $a^2 \equiv 1 \equiv b \pmod 3$, implying that $m \equiv -2ab \equiv a \pmod 3$. All of this

implies that $(\alpha^2 + m\alpha + 1)/3$ is in R. If $m \equiv -2 \pmod 3$, then we can see that $(\alpha - 1)^2/3 \in R$. Hence

$$\mathrm{Tr}\left(\frac{(\alpha-1)^2}{3}\right)^4 = \frac{28m^2 - 56m + 1}{27} \in \mathbb{Z},$$

and so $m(m-2) \equiv -1 \pmod 9$. It is easy to check that the only way this can happen is when $m \equiv 1 \pmod 9$, contradicting our assumption. A similar contradiction arises if we pick $m \equiv 2 \pmod 9$, and hence our initial assumption that $3 \mid d_2$ must have been incorrect. Now we consider the case where 3 divides m but 9 does not. Assume $3 \mid d_2$. Then 3 also divides $a^2 + 2b$ and $b^2 + 2am$. Hence $3 \mid b$ and also $3 \mid a$. Thus $\alpha^2/3$ is in R, and so $m^2/27$ is in $\mathbb{Z}$, contradicting our assumption that $9 \nmid m$. Our final case is when $9 \mid m$. Assume now that $9 \mid d_2$. Then $9 \mid b^2 + 2am$ implies $9 \mid b^2$. Then at least $3 \mid b$. Then since $9 \mid a^2 + 2b$, we have $9 \mid a^2$, which implies that $9 \mid b$ as well. But then we recall from above that $(\alpha^2 + a\alpha)/3 \in R$, and so $9^3 \mid m(m + a^3)$, which, if we stare at it long enough, leads to $9^2 \mid m$, a contradiction.

2.2.3. *The discriminant ... finally.* Although the last section was a bit technical an somewhat obscure, it none the less got the job done. Though at first it might not be apparent, we have in fact shown that

$$d_2 = \begin{cases} 3k & \text{if } m \equiv \pm 1 \pmod 9 \\ k & \text{if } m \not\equiv \pm 1 \pmod 9 \end{cases},$$

which also means that an integral basis for $\mathbb{Q}(\sqrt[3]{m})$ has the form

$$\left\{1, \alpha, \frac{\alpha^2}{k}\right\} \quad \text{when } m \equiv \pm 1 \pmod 9,$$
$$\left\{1, \alpha, \frac{\alpha^2 \pm k^2\alpha + k^2}{3k}\right\} \quad \text{when } m \not\equiv \pm 1 \pmod 9.$$

Now that we have found an integral basis, calculation of the discriminant amounts to calculating the square of the determinant of a 3×3 matrix. We will not perform this calculation here, but the result is

$$disc\left(\mathbb{Q}(\sqrt[3]{m})\right) = \begin{cases} -3kh & \text{if } m \equiv \pm 1 \pmod 9 \\ -27kh & \text{if } m \not\equiv \pm 1 \pmod 9 \end{cases}.$$

To sum up, the amount of work required to find the discriminant of even a small class of cubic extensions surpasses that which is required to determine the discriminant of all quadratic extensions, affirming the large increase in complexity associated with even a small increase in degree.

3. Quartic Extensions

Degree 4 extension are, *dans un certain sens*, the first interesting case, at least when it comes to the determination of Galois groups. This section will be entirely devoted to the classification of the Galois groups of extensions of degree 4 over $\mathbb{Q}$. There are only two groups of order 4: V, the Klein 4-group, and $\mathbb{Z}_4$, the cyclic group of order 4.

3.1. **Biquadratic Extensions.** We first consider the easiest case, i.e. when K (finite and Galois over $\mathbb{Q}$) has $G(K:\mathbb{Q}) \cong V$. The group V has two distinct subgroups of order 2, which, by the Fundamental Theorem of Galois Theory (FTGT), correspond to two distinct subfields of degree 2 over $\mathbb{Q}$. These two subfields can be written in the form $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{n})$ where $m \neq n$ and both are squarefree integers. The smallest field containing both of these is, of course, $\mathbb{Q}(\sqrt{m},\sqrt{n})$, which has degree 4 over $\mathbb{Q}$. Thus we can conclude that every extension K with Galois group over $\mathbb{Q}$ isomorphic to V is in this form. Going the other way, if we have two squarefree integers $m \neq n$, then every element of $G\big(\mathbb{Q}(\sqrt{m},\sqrt{n}):\mathbb{Q}\big)$ has at most order 2, since the only conjugate of $\sqrt{m}$ (or $\sqrt{n}$) is $-\sqrt{m}$ (or $-\sqrt{n}$). This tells us that the Galois group must be isomorphic to V, as $\mathbb{Z}_4$ has two elements of order 4.

3.2. **Cyclic Extensions.** Now the more interesting case. We approach cyclic extensions in the natural way: namely, we will view them as degree 2 extensions of quadratic extensions. Thus they will all have the form $\mathbb{Q}(\sqrt{m})(\sqrt{\alpha})$, where $\alpha \in \mathbb{Q}(\sqrt{m})$ and hence $\alpha = \sqrt{a+b\sqrt{m}}$ for some $a, b \in \mathbb{Q}$. We know that if $b = 0$, then we have a Galois extension with Galois group isomorphic to either V or $\mathbb{Z}_2$, depending on whether $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{m})$ or not. If $a = 0$, then the extension looks like $\mathbb{Q}(\sqrt[4]{d})$ (where $d = b^2m$). The conjugates of $\sqrt[4]{d}$ over $\mathbb{Q}$ are the other roots of $x^4 - b^2m$: $\zeta\sqrt[4]{d}$, $\zeta^2\sqrt[4]{d}$, and $\zeta^3\sqrt[4]{d}$, where ζ is a primitive 4^{th} root of unity. Then it is easy to see that if we are working with a Galois extension, then $i \in \mathbb{Q}(\sqrt[4]{d})$, which means that $\mathbb{Q}(i) \subset \mathbb{Q}(\sqrt[4]{d})$, and so this must be the unique quadratic subextension of degree 2 (unique by the FTGT). Hence we may assume that $m = -1$ to begin with, and so our extension is nothing more than $\mathbb{Q}(\sqrt{ib})$. Since $\sqrt{i} = \frac{1}{2}\sqrt{2} + \frac{1}{2}i\sqrt{2}$, we know that $2\sqrt{ib} = \sqrt{2b} + i\sqrt{2b}$, and hence $\mathbb{Q}(\sqrt{ib}) \subseteq \mathbb{Q}(i,\sqrt{2b})$, which means that the Galois group of $\mathbb{Q}(\sqrt{ib})$ is isomorphic to either $\mathbb{Z}_2$ or V, since the Galois group of $\mathbb{Q}(i,\sqrt{2b})$ has already been shown to be one of these. Hence we know that if we are looking for a cyclic extension, we need only consider the cases where $a \neq 0 \neq b$.

3.2.1. *Some necessary and sufficient conditions.* So let us choose $a, b \in \mathbb{Q}$, not both zero, such that $\mathbb{Q}\big(\sqrt{a+b\sqrt{m}}\big)$ is a Galois extension of $\mathbb{Q}$ (m, as usual, is

taken to be squarefree). Our field must contain, then, not only $\sqrt{a+b\sqrt{m}}$, but also $\sqrt{a-b\sqrt{m}}$, since they are conjugates (from now on we will call them α and $\bar{\alpha}$, respectively). The other two conjugates differ by only a negative sign, and so we can correctly claim that our field is a Galois extension if and only if it contains $\bar{\alpha}$. We now proceed to prove a rather general statement which can be applied to our specific case. This statement is: for a field K with *char* $K \neq 2$ and any elements $a, b \in K$, not squares in K, $K(\sqrt{a}) = K(\sqrt{b})$ if and only if $a = x^2 b$ for some $x \in K$. Let us first assume the equality of the two fields. Then $\sqrt{a} = y + z\sqrt{b}$ for some $y, z \in K$. We then get $a = y^2 + 2yz\sqrt{b} + z^2 b$. Now we can see that either $y = 0$ or $z = 0$ (but not both), or else $a \notin K$. If $z = 0$, then a is a square, contra our assumption. Hence $y = 0$ and we get $a = z^2 b$ where $z \in K$. Now assume that $a = x^2 b$ for some $x \in K$. Then $\sqrt{a} = \pm x\sqrt{b} \in K(\sqrt{b})$ and $\sqrt{b} = \pm\frac{1}{x}\sqrt{a} \in K(\sqrt{a})$. Hence $K(\sqrt{a}) = K(\sqrt{b})$.

We can apply this directly to our situation. We have $\mathbb{Q}(\alpha)$ Galois if and only if $\mathbb{Q}(\alpha) = \mathbb{Q}(\bar{\alpha})$, if and only if $\alpha = c^2\bar{\alpha}$ for some $c \in \mathbb{Q}(\sqrt{m})$, and this holds if and only if

$$\frac{a+b\sqrt{m}}{a-b\sqrt{m}} = \frac{(a+b\sqrt{m})^2}{a^2-b^2m} = c^2,$$

i.e. if and only if $a^2 - b^2 m$ is a square in $\mathbb{Q}(\sqrt{m})$, say

$$a^2 - b^2 m = (d + e\sqrt{m})^2 = d^2 + 2ed\sqrt{m} + e^2 m.$$

As before, either $d = 0$ or $e = 0$. In the latter case, we have $a^2 - b^2 m = d^2$. We will show that in this case, our extension does not have a Galois group isomorphic to $\mathbb{Z}_4$ (which is unfortunate since it is rather easy to find all solutions of this equation for a and b). First we note that $\sqrt{a^2 - b^2 m} = \bar{\alpha}\alpha = d$, and so $\alpha = d/\bar{\alpha}$. Thus if we consider any element ϕ of the Galois group, the order of ϕ can be at most 2 since this is certainly the case if ϕ takes α to $-\alpha$, and if ϕ takes α to $\bar{\alpha}$, we have

$$\phi^2(\alpha) = \phi\left(\pm\frac{d}{\alpha}\right) = \pm\frac{d}{\phi(\alpha)} = \pm\frac{d}{\pm\frac{d}{\alpha}} = \alpha,$$

and hence ϕ has order 2. Therefore, it is a necessary and sufficient condition for K to be Galois and cyclic over $\mathbb{Q}$ that $a^2 - b^2 m = e^2 m$ for some $e \in \mathbb{Q}$. We can simplify this condition by dividing through by e^2 and absorbing it into a^2 and b^2, yielding $a^2/m - b^2 = 1$.

3.2.2. *Some more on this note.* There are two basic approaches (as there are for most problems) to trying find all fields of degree 4 over $\mathbb{Q}$ with cyclic Galois group : the clever approach and brute force. We will discuss the latter approach first. The idea is that there is an easy solution to our equation, viz. $a = 0$, $b = i$, but we are not allowed to use it. However, what we *are* allowed to do is use this solution to

find other solutions. It is clear that any rational solution to this equation will lie on a line connecting the point $(0, i) \in \mathbb{C}^2$ with our solution, and that this line will have complex rational slope. Likewise, if we take any line with complex rational slope through the point $(0, i)$, we will get another complex rational solution (this is a simple algebraic computation), i.e. all solutions can be found in this way. Thus we take $b = (\frac{c}{d} + i\frac{e}{f})a + i$ for some $c, d, e, f \in \mathbb{Z}$. We may assume that none of these integers are zero, since if $c = 0$ then b is pure imaginary, and if $e = 0$ then $Imb = i$ if a is real. If we plug this into our original equation ($a^2/m - b^2 = 1$) and ask a symbolic engine to solve for a, we get

$$a = \frac{-2m(\frac{e}{f} - \frac{c}{d}i)}{\left(1 - \frac{mc^2}{d^2} - \frac{me^2}{f^2}\right) + i\frac{2mce}{df}}.$$

Again asking a symbolic engine, we find that if we require $a \in \mathbb{R}$, then $md^3f^4 - m^2df^4c^3 - md^3f^2ce^2 = 0$, an equation which can be whittled down to $d^2f^2 - mf^2c^2 - md^2e^2 = 0$ by using the fact that we are dealing with nonzero numbers. The quadratic formula then tells us that this equation holds if and only if

$$d = \pm fc\sqrt{\frac{m}{f^2 - me^2}}.$$

Since d is an integer and m is squarefree, the only way that this can happen is if $f^2 - me^2 = m$. At first it may seem that we are right back where we started, but then we realize that f and e are *integers*, i.e. we have just shown that if there is a solution the equation $a^2/m - b^2 = 1$ over the rationals, then there must also be one over the integers. This is as far as the brute force method can take us.

The clever approach leads to a different though likewise incomplete result. We again rewrite our equation as $a^2 = m(1 + b^2)$. We can show that if ζ is a primitive m^{th} root of unity, then $\sqrt{m} \in \mathbb{Q}\zeta$. For a prime p, define the *Legendre symbol* of a, $\left(\frac{c}{p}\right)$, as follows:

$$\left(\frac{c}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{otherwise} \end{cases}.$$

Now we take the *Gauss sum* of ζ, and let

$$g = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \zeta^c \in \mathbb{Q}(\sqrt{m}).$$

Looking at the complex conjugate $\bar{g}$ of g, we see that

$$\bar{g} = \sum_{c=1}^{p-1} \overline{\left(\frac{c}{p}\right) \zeta^c} = \sum_{c=1}^{p-1} \left(\frac{-c}{p}\right) \bar{\zeta}^c = \left(\frac{-1}{p}\right) g,$$

but we also have (summing over equivalence classes mod p, which we are clearly justified in doing)

$$\begin{aligned} g\bar{g} &= \left(\frac{-1}{p}\right)\sum_{a,b}\left(\frac{ab}{p}\right)\zeta^{a+b} = \left(\frac{-1}{p}\right)\sum_{a}\sum_{ab}\left(\frac{a^2b}{p}\right)\zeta^{a(1+b)} = \left(\frac{-1}{p}\right)\sum_{a,b}\left(\frac{b}{p}\right) \\ &= \left(\frac{-1}{p}\right)\sum_{a}\left(\frac{p-1}{p}\right)\zeta^{a(p-1+1)} + \left(\frac{-1}{p}\right)\sum_{a,b\neq p-1}\left(\frac{b}{p}\right)\zeta^{a(1+b)} \\ &= \left(\frac{-1}{p}\right)^2\sum_{a}1 + \left(\frac{-1}{p}\right)\sum_{b\neq p-1}\left(\frac{b}{p}\right)\sum_{a}\left(\zeta^{b+1}\right)^a \\ &= p-1+\left(\frac{-1}{p}\right)\sum_{b\neq p-1}\left(\frac{b}{p}\right)(-1) = p-\left(\frac{-1}{p}\right)\left(\left(\frac{-1}{p}\right)+\sum_{b\neq p-1}\left(\frac{b}{p}\right)\right) \\ &= p-\left(\frac{-1}{p}\right)\sum_{b=1}^{p-1}\left(\frac{b}{p}\right) = p, \end{aligned}$$

and hence $|g| = p$. The fact that $\bar{g} = \pm g$ tells us then that $g = \sqrt{\pm p}$.

Since we will only be interested in primes p equivalent to 1 mod 4, we assume now that $p \equiv 1 \pmod 4$ and thus $\left(\frac{-1}{p}\right) = 1$ (the easiest way to see that this is true is to note that in this case $\mathbb{Z}_{p-1} \cong \mathbb{Z}_p^\times$ has an element of order 4). So now we have $g = \sqrt{p}$, implying that $\sqrt{p} \in \mathbb{Q}(\zeta)$. Moreover, the (cyclic) Galois group of $\mathbb{Q}(\zeta)$ has degree divisible by 4, and so by the FTGT we know that there is a unique degree 4 cyclic subextension, necessarily containing $\mathbb{Q}(\sqrt{p})$ since this is the unique subextension of degree 2. If $m = p_1 \dots p_n$ where $p_i \equiv 1 \pmod 4$, then if ζ is a primitive m^{th} root of unity the Galois group of $\mathbb{Q}(\zeta)$ is isomorphic to $\mathbb{Z}_{p_1-1} \times \dots \times \mathbb{Z}_{p_n-1}$. Let us consider the subgroup of order 2 generated by the element $\big((p_1-1)/2, \dots, (p_n-1)/2\big)$. We can choose ζ to be the product $\zeta_{p_1} \dots \zeta_{p_n}$ where ζ_{p_i} is a primitive p_i^{th} root of unity. It is clear that we can view each factor of $\mathbb{Z}_{p_i-1}$ in the Galois group of $\mathbb{Q}(\zeta)$ as corresponding to the subfield of $\mathbb{Q}(\zeta_{p_i})$. Doing this also makes it clear that each subfield generated by $\big(0, \dots, (p_i-1)/2, 0, \dots\big)$ contains $\sqrt{p_i}$. Hence the subfield in consideration contains $\sqrt{m}$, and is, in fact, $\mathbb{Q}(\sqrt{m})$. This allows us to find a large class of examples of cyclic extensions of degree 4, which can be quite a useful, and at least tells us that there infinitely many such extensions.

3.2.3. *Further possibilities.* The main point to keep in mind when looking for extensions of degree a higher power of 2 is that most of the work is done in characterizing the next lowest power. Groups of order 2^n will always have subgroups of order 2^{n-1}, and will often be largely determined by them. Thus, once all fields of degree 2^{n-1} have been classified, it becomes much easier to classify fields of the next highest

degree. For example, the work done in this paper can be used directly to find all fields of degree 8 whose Galois group is isomorphic either to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ or to $\mathbb{Z}_4 \times \mathbb{Z}_2$. Adding a factor of 3 into the degree of the field is likewise relatively straightforward.

References

[1] Larry Grove, *Algebra*, Academic Press, San Diego, 1983.

[2] Serge Lang, *Algebraic number theory*, Addison-Wesley, Menlo Park, CA, 1970.

[3] Daniel A. Marcus, *Number fields*, Springer-Verlag, New York, 1977.