Notes on Quadratic Extension Fields

1 Standing notation

- $\mathbf{Q}$ denotes the field of rational numbers.
- $\mathbf{R}$ denotes the field of real numbers.
- $\mathbf{F}$ always denotes a subfield of $\mathbf{R}$.
- The symbol k is always a positive real number that is in $\mathbf{F}$. *but whose square root is not in* $\mathbf{F}$.
- $\mathbf{F}(\sqrt{\mathbf{k}})$ is defined to be the collection of all real numbers of the form $a + b\sqrt{k}$, where a and b belong to $\mathbf{F}$. We call $\mathbf{F}(\sqrt{\mathbf{k}})$ a *quadratic extension of* $\mathbf{F}$.

2 Basic properties of quadratic extensions

According to Problem 15 of Chapter 15, $\mathbf{F}(\sqrt{\mathbf{k}})$ is a subfield of $\mathbf{R}$ that contains $\mathbf{F}$. Since $\sqrt{k}$ belongs to $\mathbf{F}(\sqrt{\mathbf{k}})$, but not to $\mathbf{F}$, we see that $\mathbf{F}(\sqrt{\mathbf{k}})$ is strictly larger than $\mathbf{F}$.

To keep things straight in your mind, you should think of the special case $\mathbf{F} = \mathbf{Q}$ and $k = 2$, so $\mathbf{F}(\sqrt{\mathbf{k}}) = \mathbf{Q}(\sqrt{\mathbf{2}})$.

Recall also that we showed in class:

Proposition 1 *Every subfield of* $\mathbf{R}$ *contains* $\mathbf{Q}$.

Proof. If $\mathbf{F}$ is a subfield of $\mathbf{R}$, then $1 \in \mathbf{F}$, hence so is $1 + 1 = 2, 1 + 2 = 3, \ldots,$ so every positive integer is in $\mathbf{F}$. Since $\mathbf{F}$ is closed under additive inverse, it contains all the integers. Since $\mathbf{F}$ is a *subfield* of $\mathbf{R}$ it contains the inverse of every non-zero integer, and therefore every quotient of integers (with non-zero denominator). In other words, $\mathbf{F}$ contains every rational number. ///

We need to know a couple of things about the representation of elements $A \in \mathbf{F}(\sqrt{\mathbf{k}})$ by "coordinates" in $\mathbf{F}$.

Proposition 2 *Suppose $A = a + b\sqrt{k}$, where a and b are in $\mathbf{F}$. Then:*

1. $A \in \mathbf{F} \iff b = 0$
2. $A = 0 \iff a = b = 0$.

Proof of 1). We did this in class. Clearly $b = 0 \Rightarrow A = a \in \mathbf{F}$. In the other direction, if $a \in \mathbf{F}$ then b must be 0. For if not then $\sqrt{k} = b^{-1}(A - a)$, which is in $\mathbf{F}$, contradicting the hypothesis that this is not so.

Proof of 2). Suppose $a + b\sqrt{k} = 0$. We're supposed to show that $a = b = 0$. Easy enough: the hypothesis tells us in particular that $a + b\sqrt{k} \in \mathbf{F}$, so by part (1) $b = 0$. Therefore also $a = 0$. ///

EXERCISE 1. Show that the both parts of the last proposition fail if $\sqrt{k}$ is in F (take $\mathbf{F} = \mathbf{Q}$ and $k = 4$, for example).

EXERCISE 2. Prove the following generalization of part (2) of the last proposition: Suppose $A_1 = a_1 + b_1\sqrt{k}$ and $A_2 = a_2 + b_2\sqrt{k}$. Then $A_1 = A_2 \iff 1 = a_2$ and $b_1 = b_2$. Explain why this justifies thinking of elements a and b of F as "coordinates" that represent $A = a + b\sqrt{k} \in \mathbf{F}(\sqrt{\mathbf{k}})$.

3 Conjugation in quadratic extensions

For each element $A = a + b\sqrt{k} \in \mathbf{F}(\sqrt{\mathbf{k}})$ we define $\overline{A} = a - b\sqrt{k}$. The corresponding operation on complex numbers ($\overline{a + bi} = a - bi$) is called *complex conjugation.* For this reason, let's agree to call $\overline{A}$ the *conjugate* of A (note that the field of complex numbers can be regarded as $\mathbf{R}(\sqrt{-\mathbf{1}})$. For homework you proved:

Proposition 3 *For any two elements A and B in $\mathbf{F}(\sqrt{\mathbf{k}})$:*

- $\overline{A + B} = \overline{A} + \overline{B}$.
- $\overline{A - B} = \overline{A} - \overline{B}$.
- $\overline{AB} = \overline{A}\ \overline{B}$.
- $\overline{A} = A \iff A \in \mathbf{F}$.

EXERCISE 3. Prove that, in addition to the above,

- $\overline{A^{-1}} = \overline{A}^{\,-1}$.
- $\overline{A/B} = \overline{A}/\overline{B}$.

Proposition 3 has important consequences. To begin with, note that upon setting $A = B$ in the third of its statements, we see that $\overline{A^2} = \overline{A}^2$. Repeating with $B = A^2$ yields $\overline{A^3} = \overline{A}^3$. Keeping on, we achieve: $\overline{A^n} = \overline{A}^n$ for any positive integer n.

EXERCISE 4. Apply this last achievement, along with Proposition 3 to any polynomial $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. *with coefficients* $a_0, a_1, \ldots a_n$ *in* $\mathbf{F}$. The result is: For ever $A \in \mathbf{F}(\sqrt{\mathbf{k}})$:

$$\overline{p(A)} = p(\overline{A}).$$

This last exercise proves:

Proposition 4 *If $p(x)$ is a polynomial with coefficients in $\mathbf{F}$, and $A \in \mathbf{F}(\sqrt{\mathbf{k}})$ is a root of p (meaning: $p(A) = 0$), then $\overline{A}$ is also a root of p.*

This result is exactly analogous to one you learn in high school: *The complex roots of a polynomial with real coefficients come in conjugate pairs.* It was hinted at in our proof that $\sqrt[3]{2}$ is not constructible. Recall that in the course of doing this we proved:

$$\sqrt[3]{2} = a + b\sqrt{k} \Rightarrow \sqrt[3]{2} = a - b\sqrt{k}.$$

EXERCISE 5. Prove that this last statement is equivalent to: If $a + b\sqrt{k}$ is a root of the polynomial $x^3 - 2$, then so is $a - b\sqrt{k}$ (Warning: This polynomial has *three roots*. Use Calculus to sketch its graph in the $x - y$ plane, and show that only one of these roots is real).

In other words, Proposition 4, along with the last exercise, gives another way of getting at the proof, done in class, that if $\sqrt[3]{2}$ belongs to $\mathbf{F}(\sqrt{\mathbf{k}})$, then it actually belongs to $\mathbf{F}$.

4 Roots in a quadratic extension

Now we're going to use Proposition 4 to generalize our last observation about $x^3 - 2$ to arbitrary cubic polynomials with coefficients in $\mathbf{F}$.

Theorem 1 *Suppose $p(x)$ is a cubic polynomial with coefficients in $\mathbf{F}$. If $p(x)$ has a root in $\mathbf{F}(\sqrt{\mathbf{k}})$, then it has a root in $\mathbf{F}$.*

Warning. Our Theorem does *not* say that *every* root of $p(x)$ that lies in $\mathbf{F}(\sqrt{\mathbf{k}})$ has to lie in $\mathbf{F}$. It says that as soon as some root lies in $\mathbf{F}(\sqrt{\mathbf{k}})$, then we know that some *possibly different one* lies in $\mathbf{F}$.

EXAMPLE. Suppose $p(x) = x^3 - x^2 - 2x + 2$. This polynomial has coefficients in $\mathbf{F} = \mathbf{Q}$, and you can easily check that $\sqrt{2}$ is a root. So $p(x)$ has a root in $\mathbf{Q}(\sqrt{\mathbf{2}})$, hence by the Theorem, it has one in $\mathbf{Q}$.

Remark. The mystery associated with this example dissolves once we realize that $p(x)$ is just $(x^2 - 2)(x - 1)$, in disguise.

Proof of Theorem. Since $p(x)$ is a cubic polynomial, its leading coefficient (the one that multiplies the x^3 term) is not zero. Suppose for the moment that this coefficient is 1. Thus $p(x) = x^3 + \alpha x^2 + \beta x + \gamma$ where $\alpha, \beta, \gamma \in \mathbf{F}$. Our hypothesis is that $A = a + b\sqrt{k}$ $(a, b \in \mathbf{F})$ is a root of $p(x)$. We want to show that some (possibly different) root lies in $\mathbf{F}$. If $b = 0$, then $A = a \in \mathbf{F}$, and we have found our root.

So suppose $b \neq 0$. In this case, Proposition 4 insures us that $\overline{A} = a - b\sqrt{k}$ is also a root of $p(x)$. Now we have two roots of a cubic polynomial. At this point, some of the theory of polynomials you learn from high school algebra comes into play, namely:

- *Every polynomial of degree n, with leading coefficient 1 can be factored as a product $(x - x_1)(x - x_2) \ldots (x - x_n)$ where $x_1.x_2, \ldots x_n$ are the (possibly complex, possibly not distinct) roots of the polynomial.*

- *If a polynomial has real coefficients, then its complex roots occur in conjugate pairs ($a \pm ib$ where $a, b \in \mathbf{R}$).*

Note that this last fact is just a version of Proposition 4 for the situation $\mathbf{C} = \mathbf{R}(\sqrt{-1})$, where $\mathbf{C}$ denotes the field of complex numbers. The proof is *exactly* the same.

Back to business! We know that A and $\overline{A}$ are two different real roots of the cubic polynomial $p(x)$. By the high school algebra review of the last paragraph, there must be a third root, C, and it must be *real* (if it were not, then there would be a fourth root $\overline{C}$ (distinct from C since C is not real) which, by the first item in our high school review, would contradict the fact that $p(x)$ is a cubic polynomial).

We claim that C is in $\mathbf{F}$! Once done, the proof is over!

To see this, write $p(x)$ as a product of linear factors involving its three distinct roots (cf. High School Review above):

$$\begin{aligned} p(x) &= (x-A)(x-\overline{A})(x-C) \\ &= (x-(a+b\sqrt{k}))(x-(a-b\sqrt{k}))(x-C) \\ &= (x^2-2ax+a^2-b^2k)(x-C) \\ &= x^3+(-2a-C)x^2+(2aC+a^2-b^2k)x-C(a^2-b^2k). \end{aligned}$$

Now recall that the coefficients of $p(x)$ all lie in $\mathbf{F}$, so from the last line above, $C(a^2-b^2k) \in \mathbf{F}$. Now $a^2-b^2k \neq 0$ (since otherwise, recalling that $b \neq 0$, we'd have the contradiction: $\sqrt{k} = a/b \in \mathbf{F}$). Thus $C \in \mathbf{F}$, which is just what we wanted to prove.

Just one minor technicality remains. We assumed our polynomial $p(x)$ has leading coefficient 1. If it does not, just divide through by the leading coefficient (which is not zero because the polynomial is assumed to be cubic), and rename the new polynomial, which now has leading coefficient 1, $p(x)$. The new polynomial and the old one have the same roots, and the argument above applies to the new one. ///

EXERCISE 6. Show (by finding counter-examples) that the Theorem does *not* hold for second and fourth degree polynomials.

Now we can apply our Theorem to constructibility problems.

Theorem 2 (Theorem 15.9 of the text.) *If a cubic polynomial with rational coefficients has a* constructible *root, then it has a* rational *root.*

Proof. Suppose $p(x)$ is such a cubic polynomial with coefficients in the field $\mathbf{Q}$, and that $p(x)$ has a constructible root a. By Theorem 15.6 (the main result of the last week or so), there is a chain of subfields of $\mathbf{R}$

$$\mathbf{Q} = \mathbf{F_1} \subset \mathbf{F_2} \subset \cdots \subset \mathbf{F_{n-1}} \subset \mathbf{F_n}$$

with each subfield a quadratic extension of the previous one, and $a \in \mathbf{F_n}$. By our Theorem, p(x) has a (possibly different) root in $\mathbf{F_{n-1}}$. Rename this root a and repeat the last sentence, with $\mathbf{F_{n-1}}$ in place of $\mathbf{F_n}$. Keep going until you get down to $\mathbf{F_1} = \mathbf{Q}$. Conclusion: $p(x)$ has a root in $\mathbf{Q}$. ///

In order to *use* this result in a systematic way, we need a theorem that tells us when a polynomial with rational coefficients has no rational roots. For example, the polynomials $x^2 - 2$ and $x^3 - 2$ have rational coefficients, but no rational roots (although you should be aware that we haven't yet proved this last fact in this course!). The result that makes it all work is Theorem 4.16 of the text:

Theorem 3 (The Rational Root Theorem) *Suppose a polynomial with integer coefficients has a rational root r/s (here r and s are integers with no common factor). Then r divides the constant coefficient of the polynomial, and s divides the leading one (the coefficient of the highest order term).*

Proof. Pages 100 - 101 of the text.

Now let's apply our machinery to get systematic solutions to two of the classical constructibility problems.

Corollary 1 (Impossible to double the cube.) $\sqrt[3]{2}$ *is not constructible.*

Proof. Suppose $\sqrt[3]{2}$ were constructible. It's a root of the polynomial $x^3 - 2$, which has rational coefficients, so by Theorem 2 this polynomial would have to have a rational root. Certainly 0 is not a root, so by the Rational Root Theorem, the only possibile rational roots are r/s where $0 \neq r|2$ and $0 \neq s|1$. That is: $r = \pm 1 \text{or} \pm 2$ and $s = \pm 1$. So the only possible rational roots of $x^3 - 2$ are $\pm 1 \text{and} \pm 2$. Clearly these are *not* roots, so the polynomial has no rational roots.

Remark. The last part of this argument shows something that we've been assuming is obvious, but haven't proved before: namely that $\sqrt[3]{2}$ is not rational.

Corollary 2 (Impossible to trisect $60°$ angle) *The polynomial $x^3 - 3x - 1$ has no constructible roots.*

Proof. The polynomial has rational coefficients, so by Theorem 2, if it had a constructible root, it would have a rational one. By the Rational Root Theorem, the only possible nonzero rational roots are 1 and -1, which are not roots. Zero is clearly not a root, so this polynomial has no rational roots, and therefore no constructible ones, either. ///

5 Impossibility of squaring the circle

The third of the classical construction problems is: *Given a circle, can you construct, with straightedge and compass alone, the square with the same area?* In this section we are going to show that the answer is *NO.*

To see what's at stake algebraically, let's suppose the circle we're given has radius 1, so its area is π. Then the square to be constructed must have edge length $\sqrt{\pi}$. Since a number is constructible if and only if its square is constructible (do you remember why this is true?), we see that the desired square can be constructed if and only if π is a constructible number.

We are going prove the following result, which, in view of what we've just said, shows that it is not possible to square the circle.

Theorem 4 *π is not a constructible number.*

To get oriented before starting the proof, let's recall how we carried out previous proofs that certain numbers a (specifically, $a = \sqrt[3]{2}, a = \cos 20°$) are not constructible. There were three basic steps:

- Show a to be a root of some cubic polynomial with integer coefficients.
- Show that this cubic polynomial has no rational roots.
- Use the caracterization of constructible numbers by quadratic extensions, and the result about roots of polynomials that lie in a quadratic extension, to conclude that if the polynomial in question had a constructible root, then it would also have a rational root.

Unfortunately, we can't even get started on this program for $a = \pi$. The reason lies in the following theorem, proved by Lindemann in the 1870's.

Theorem 5 ("Transcendence" of π.) *There is no polynomial with integer coefficients that has π as a root.*

This result lies deeper than anything we've done in this class, and we're not going to prove it[1]. The terminology comes from the fact that any root of a polynomial with integer coefficients is called an *algebraic* number, while a number that's not algebraic (i.e. a root of *no* such polynomial)is called *transcendental.* Thus, Theorem 5 can be rephrased: *π is transcendental.*

Although Theorem 5 shoots down our previous method for showing numbers to be non-constructible, it allows us to use another method, whose foundation is the next result. As usual, $\mathbf{F}$ is a subfield of the real numbers, and $\mathbf{F}(\sqrt{\mathbf{k}})$ a quadratic extension of $\mathbf{F}$ $(\mathbf{0} < \mathbf{k} \in \mathbf{F}, \sqrt{\mathbf{k}} \notin \mathbf{F})$.

[1] If you'd like to browse through a proof that uses nothing more than Calculus, see Hadlock's little monograph *Field Theory and its Classical Problems*, which is on reserve in the Math. Library.

Theorem 6 *Suppose $a \in \mathbf{R}$ is a root of a polynomial with coefficients in $\mathbf{F}(\sqrt{\mathbf{k}})$. Then a is also a root of some polynomial with coefficients in $\mathbf{F}$.*

Discussion of Theorem. To get some feeling for this result, consider $a = \sqrt{2}$, which is a root of the first degree polynomial $x - \sqrt{2}$, that has coefficients in the field $\mathbf{Q}(\sqrt{2})$. Theorem 6 asserts that $\sqrt{2}$ is a root of some other polynomial with coefficients in $\mathbf{Q}$, and indeed it is: it's a root of $x^2 - 2$.

Proof of Theorem 6. Suppose a is a root of the polynomial

$$p(x) = A_n x^n + A_{n-1}x^{n-1} + \ldots + A_1 x + A_0,$$

where the coefficients $A_0, A_1, \ldots A_n$ all belong to $\mathbf{F}(\sqrt{\mathbf{k}})$. Thus for $j = 0, 1, 2, \ldots, n$, we have

$$A_j = \alpha_j + \beta_j \sqrt{k},$$

where $\alpha_j, \beta_j \in \mathbf{F}$. Since a is a root of $p(x)$, we have

$$0 = p(a) = (\alpha_n + \beta_n\sqrt{k})a^n + (\alpha_{n-1} + \beta_{n-1}\sqrt{k})a^{n-1} + \ldots + (\alpha_1 + \beta_1\sqrt{k})a + (\alpha_0 + \beta_0\sqrt{k}).$$

Now transfer all the terms containing $\sqrt{k}$ to the other side of the equation, to get

$$\alpha_n a^n + \alpha_{n-1}a^{n-1} + \ldots + \alpha_1 a + \alpha_0 = -\sqrt{k}(\beta_n a^n + \beta_{n-1}a^{n-1} + \ldots + \beta_1 a + \beta_0).$$

Square both sides of this last equation. You needn't do the whole calculation; just convince yourself that the result is

$$p_1(a) = kp_2(a),$$

where p_1 and p_2 are polynomials with coefficients in $\mathbf{F}$ ($p_1(x)$ is the square of the polynomial you get by replacing the coefficient A_j in the definition of $p(x)$ by $\alpha_j, 0 \leq j \leq n$, and similarly for p_2, with β in place of α). Thus a is a root of the polynomial $q(x) = p_1(x) - kp_2(x)$, which (since $k \in \mathbf{F}$) also has coefficients in $\mathbf{F}$. ///

EXERCISE 7. Observe that both polynomials $p_1(x)$ and $p_2(x)$ have degree at most $2n$, and at least one of them has degree exactly $2n$. Thus $q(x)$ has degree at most $2n$. Show that the degree of q is, in fact, exactly $2n$.

Proof of Theorem 4. Our goal is to show that π is not constructible. Suppose otherwise. By the fundamental characterization of constructible numbers, there is a chain of subfields of $\mathbf{R}$

$$\mathbf{Q} = \mathbf{F_1} \subset \mathbf{F_2} \subset \cdots \subset \mathbf{F_{n-1}} \subset \mathbf{F_n}$$

with each subfield a quadratic extension of the previous one, and $\pi \in \mathbf{F}_n$. Thus the polynomial $x - \pi$, which has π as a root, has both of its coefficients in $\mathbf{F}_n$, hence by Theorem 6 there is a polynomial with coefficients in $\mathbf{F}_{n-1}$ that has π as a root. Apply Theorem 6 to this new situation, obtaining a polynomial with coefficients in $\mathbf{F}_{n-2}$ and having π as a root. Continuing in this manner, we ultimately conclude that some polynomial with rational coefficients has π as a root, hence (upon multiplying this polynomial through by the product of the coefficient denominators) the same is true of some polynomial with integer coefficients. But this contradicts Lindemann's Theorem (Theorem 5). The contradiction originated with our assumption that π is constructible. Thus π is not constructible, as we wished to prove. ///