Three Examples

In all our examples the ground field shall be \( Q \) and the extension field will be a subfield of the complex numbers \( C \).

We take as basic that the only nonzero rational numbers \( c \) for which \( \sqrt{c} \in Q \) are those positive \( c \) for which each prime factor \( p \) appears an even number of times. In particular, \( \sqrt{2}, \sqrt{3}, \sqrt{3/2} \) are all irrational.

**Example 1:** \( K = Q(\sqrt{2}, \sqrt{3}) \).

As \( \sqrt{2} \) has minimal polynomial \( x^2 - 2 \), \( Q(\sqrt{2}) \) has basis \( 1, \sqrt{2} \) over \( Q \).

Now we need a simple result:

**Theorem 0.1** \( \sqrt{3} \notin Q(\sqrt{2}) \)

**Proof:** If it were we would have

\[
\sqrt{3} = a + b\sqrt{2}
\]

with \( a, b \in Q \). Squaring both sides

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

As \( 1, \sqrt{2} \) is a basis the coefficient of \( \sqrt{2} \) would need be zero. That is, \( 2ab = 0 \). So either \( a = 0 \) or \( b = 0 \).

1. \( b = 0 \): Then \( \sqrt{3} = a \in Q \), contradiction.

2. \( a = 0 \). Then \( \sqrt{3} = b\sqrt{2} \) so \( 3\sqrt{2} = b \in Q \), contradiction.

From Theorem 0.1 and that \( \sqrt{3} \) satisfies a quadratic (namely, \( x^2 - 3 \)) over \( Q(\sqrt{2}) \), \( 1, \sqrt{3} \) is a basis for \( Q(\sqrt{2}, \sqrt{3}) \) over \( Q(\sqrt{2}) \) and so \( 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \) is a basis for \( K \) over \( Q \). That is, we may write

\[
K = Q(\sqrt{2}, \sqrt{3}) = \{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in Q \} \tag{1}
\]

and every \( \alpha \in K \) has a unique expression in this form.

Now we turn to the Galois Group \( \Gamma(K : Q) \). Any \( \sigma \in K \) has \( \sigma(\sqrt{2}) = \pm\sqrt{2} \) and \( \sigma(\sqrt{3}) = \pm\sqrt{3} \) which gives four (Caution: this is \( 2 \) times \( 2 \)) possibilities. The value of \( \sigma \) on \( \sqrt{2}, \sqrt{3} \) determines the value on all of \( K \). The four elements of the Galois Group are \( e, \sigma_1, \sigma_2, \sigma_3 \) where

\[
e(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}
\]

\[
\sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}
\]

1
\[
\sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\
\sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}
\]

**Exercise:** Check that these really are automorphisms, that they are bijections (easy!) that send sums to sums (easy!) and products to products (a bit messier!). This will actually come out of more general stuff later.

What does the group \(\Gamma(K : Q)\) look like. The identity is the identity, no problem. Any \(\sigma\) when squared gives the identity. For example

\[
\sigma_1^2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = \sigma_1(a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}
\]

We can also see this by noticing that either \(\sigma(\sqrt{2}) = \sqrt{2}\) or \(\sigma(\sqrt{2}) = -\sqrt{2}\) but in either case \(\sigma^2(\sqrt{2}) = \sqrt{2}\) and similarly \(\sigma^2(\sqrt{3}) = \sqrt{3}\) so that \(\sigma^2 = e\). We also calculate that if you multiply any two of \(\sigma_1, \sigma_2, \sigma_3\) in either direction you get the other third one. For example

\[
\sigma_2(\sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})) = \sigma_2(a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}
\]

We have the Klein Vierergruppe, aka the Fourgroup, which is isomorphic to \(Z_2 \times Z_2\). Actually, there are only two groups with four elements (up to isomorphism, of course), the cyclic group \(Z_4\) and the Vierergruppe \(Z_2 \times Z_2\) so once it isn’t the first it must be the second!

**Example II:** \(K = Q(\epsilon)\) with \(\epsilon = e^{2\pi i/5}\). \(\epsilon\) satisfies \(x^5 - 1 = 0\) and, as \(\epsilon \neq 1\), it satisfies \(p(x) = 0\) with

\[
p(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1
\]

This is irreducible (one can show this by replacing \(x\) by \(x + 1\) giving \(x^4 + 5x^3 + 10x^2 + 5x + 5\) and using Eisenstein’s criterion) so \([K : Q] = 4\) and we write

\[
K = \{a + b\epsilon + c\epsilon^2 + d\epsilon^3 : a, b, c, d \in Q\}
\]

The minimal polynomial \((2)\) has roots \(\epsilon, \epsilon^2, \epsilon^3, \epsilon^4\). From our general results (earlier notes) the Galois Group \(\Gamma(K : Q)\) consists of four automorphisms which we shall label \(\sigma_1, \sigma_2, \sigma_3, \sigma_4\). They are determined by their values on \(\epsilon\) and we shall let \(\sigma_j\) be that automorphism with \(\sigma_j(\epsilon) = \epsilon^j\). Note that \(\sigma_1\) is the identity and \(\sigma_4\) is our old friend, complex conjugation.

What is the product \(\sigma_j \sigma_k\)? Let’s see what it does to \(\epsilon\).

\[
(\sigma_j \sigma_k)(\epsilon) = \sigma_j(\sigma_k(\epsilon)) = \sigma_j(\epsilon^k) = \sigma_j(\epsilon)^k = (\epsilon^j)^k = \epsilon^{jk}
\]

Hmmm, so it looks like \(\sigma_j \sigma_k = \sigma_{jk}\). But we only have four automorphisms. What does it mean to say \(\sigma_3 \sigma_3 = \sigma_9\)? The key is that \(\epsilon^5 = 1\) so that we can reduce \(\epsilon^{jk}\) by reducing \(jk\) modulo 5. As \(\epsilon^9 = \epsilon^4\) we have \(\sigma_3 \sigma_3 = \sigma_4\). So we can and do say \(\sigma_j \sigma_k = \sigma_{jk}\) with the understanding that \(jk\) is computed modulo 5. With this we have

\[
\Gamma(K : Q) \cong Z_5^*
\]

where we associate \(\sigma_j\) with \(j\). Finally \(Z_5^* \cong \{1, 2, 3, 4\}\) (the cyclic group, not the Vierergruppe) be associating 1, 2, 3, 4 with 0, 1, 3, 2 respectively.

**Example III:** \(K = Q(2^{1/3}, \omega)\) with \(\omega = e^{2\pi i/3}\). Monday