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** $\sqrt{3} \not\in Q(\sqrt{2})$

**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 $\sqrt{3/2} = b \in Q$, 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

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

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

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

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

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

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

**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 it mean to say that \( \sigma \) is an automorphism? We have the Klein Vierergruppe, aka the Fourgroup, which is isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \). Actually, there are only two groups with four elements (up to isomorphism, of course), the cyclic group \( \mathbb{Z}_4 \) and the Vierergruppe \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) 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 \( x^4 + 5x^3 + 11x^2 + 5x + 5 \) 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 \( \epsilon \).
\[
(\sigma_j \sigma_k)(\epsilon) = \sigma_j(\sigma_k(\epsilon)) = \sigma_j(\epsilon^k) = \sigma_j(\epsilon)^k = (\epsilon^j)^k = \epsilon^{jk}
\]

Hmmmm, 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
\[
\Gamma(K : Q) \cong \mathbb{Z}_5^*
\]

where we associate \( \sigma_j \) with \( j \). Finally \( \mathbb{Z}_5^* \cong (\mathbb{Z}_4, +) \) (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 \( \omega = e^{2\pi i/3} \).

The polynomial
\[
p(x) = x^3 - 2
\]  
(6)
is irreducible (by Eisenstein’s criterion, or simply that, as a cubic, it has no rational roots) and its roots are \( \alpha, \beta, \gamma \) where for convenience we write
\[
\alpha = 2^{1/3}, \beta = 2^{1/3} \omega, \gamma = 2^{1/3} \omega^2
\]  
(7)
Any field that contains \( 2^{1/3}, \omega \) contains \( \alpha, \beta, \gamma \) and any field that contains \( \alpha, \beta, \gamma \) contains \( 2^{1/3}, \omega \) so we may also write \( K = Q(\alpha, \beta, \gamma) \), so \( K \) is the splitting field (to be defined later) of \( p(x) \) over \( Q \). A basis for \( Q(\alpha) \) over \( Q \) is \( 1, \alpha, \alpha^2 \). As all elements of \( Q(\alpha) \) are real, \( \omega \not\in Q(\alpha) \). As \( \omega \) satisfies the quadratic \( 1 + x + x^2 = 0 \) over \( Q(\alpha) \), a basis for \( K = Q(\alpha, \omega) \) over \( Q(\alpha) \) is \( 1, \omega \). Hence a basic for \( K \) over \( Q \) is \( 1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2 \) and we can write
\[
K = \{ a + b\alpha + c\alpha^2 + d\omega + e\omega\alpha + f\omega\alpha^2 : a, b, c, d, e, f \in Q \} \]  
(8)
and each \( \zeta \in K \) has a unique such representation.

What are the automorphisms \( \sigma \in \Gamma(K : Q) \)? As \( K = Q(\alpha, \beta, \gamma) \), \( \sigma \) is determined by its values on \( \alpha, \beta, \gamma \). Further, as \( \alpha, \beta, \gamma \) satisfy the same irreducible (6), \( \sigma \) of any of them must be one of them. Further, as \( \sigma \) must be a bijection, \( \sigma \) cannot send two of \( \alpha, \beta, \gamma \) to the same value and hence \( \sigma \) must be a permutation on \( \alpha, \beta, \gamma \). This gives that there are at most six automorphisms and that \( \Gamma(K : Q) \) is isomorphic to a subgroup of \( S_3 \), the full symmetric group on three elements, here \( \alpha, \beta, \gamma \).

Actually, all permutations of \( \alpha, \beta, \gamma \) yield automorphisms of \( K \) and so
\[
\Gamma(K : Q) \cong S_3
\]  
(9)
This actually will follow from some general stuff but we can give an idea here. Two automorphisms are easy, the identity (we always have the identity) and complex conjugation \( \sigma \). We do have to check that complex conjugation is a bijection from \( K \) to itself. As \( \sigma(\alpha) = \alpha \) and \( \sigma(\omega) = \omega^2 \in K \) it sends \( K \) to \( K \) and since \( \sigma^2 = e \) it must be a bijection. (That is, \( \sigma^{-1}(\zeta) = \sigma(\zeta) \).) This \( \sigma \) corresponds to the permutation that keeps \( \alpha \) fixed and transposes \( \beta, \gamma \).

Here is another \( \tau \in \Gamma(K : Q) \). Generate it by setting \( \tau(\alpha) = \beta \) and \( \tau(\omega) = \omega \). Then
\[
\tau(\beta) = \tau(\alpha\omega) = \tau(\alpha)\tau(\omega) = \beta\omega = \gamma
\]  
(10)
and
\[
\tau(\gamma) = \tau(\beta\omega) = \tau(\beta)\tau(\omega) = \gamma\omega = \alpha
\]  
(11)
so it cycles \( \alpha \) to \( \beta \) to \( \gamma \) back to \( \alpha \). With the representation of (8)
\[
\tau(a + b\alpha + c\alpha^2 + d\omega + e\omega\alpha + f\omega\alpha^2) = a + b\omega\alpha + c\omega^2\alpha^2 + d\omega + e\omega^2\alpha + f\alpha^2
\]  
(12)
In this form (but, like I said, there are other approaches) one need show \( \tau \) is bijective (pretty easy), that \( \tau(\zeta_1 + \zeta_2) = \tau(\zeta_1) + \tau(\zeta_2) \) (quite easy), and that \( \tau(\zeta_1\zeta_2) = \tau(\zeta_1)\tau(\zeta_2) \) (lengthy, unless you use some tricks).
Indeed, here is another approach to show that $\tau$ is indeed an automorphism from $K$ to $K$. Consider the intermediate field $L = Q(\omega)$. We first claim that $p(x)$ given by (6) is irreducible over $L$. As it is a cubic, if it reduced it would have a root in $L$. So either $\alpha, \beta = \alpha \omega, \gamma = \alpha \omega^2$ would be in $L$. As $\omega \in L$ if any of $\alpha, \beta, \gamma$ were in $L$ then all three would be in $L$, in particular $\alpha \in L$. But then $L$ would have $\omega$ and $\alpha$ and so would be $Q(\alpha, \omega) = K$. As $[L : Q] = 2 \neq 6 = [K : Q]$ that cannot happen. Now $\alpha, \beta$ have the same minimal polynomial in $L[x]$ and $K = L(\alpha) = L(\beta)$, so, from the previous notes, there does exist an automorphism $\tau$ of $K$ that preserves $L$ and has $\tau(\alpha) = \beta$. As it preserves $L$ we also have $\tau(\omega) = \omega$. Since $\tau$ preserves $L$ it certainly preserves the smaller $Q$ and so $\tau \in \Gamma(K : Q)$.

Once we have $\sigma, \tau \in \Gamma(K : Q)$ we have that $\Gamma(K : Q)$ is a subgroup of $S_3$ that contains an element $\tau$ of order three and an element $\sigma$ of order two. From $\tau$ it must have at least three elements, from $\sigma$ it can’t have exactly three elements, so it has more than three elements, so it has all six elements, it is all of $S_3$. 