§ 10 Some extensions of small degree

Proposition 10.1 Let K be a field and let L be an extension of K of degree two.

(a) There is an element $\alpha \in L \setminus K$ such that $L = K(\alpha)$ and $\alpha^2 \in K$.

(b) The element α has the following uniqueness property: if $L = K(\beta)$ for some other element $\beta \in L \setminus K$ with $\beta^2 \in K$, then $\beta = q\alpha$ for some $q \in K$.

(c) There is an automorphism $\sigma\colon L \to L$ that acts as the identity on K and satisfies $\sigma(\alpha) = -\alpha$.

(d) We have $\sigma^2 = 1$ and $\mathrm{Gal}(L/K) = \{1, \sigma\} \simeq C_2$.

PROOF: First choose any element $\lambda \in L \setminus K$. We claim that 1 and λ are linearly independent over K. To see this, consider a linear relation $a.1 + b\lambda = 0$ with $a, b \in K$. If $b \neq 0$ we can rearrange to get $\lambda = -ab^{-1} \in K$, contrary to assumption. We therefore have $b = 0$ so the original relation reduces to $a = 0$ as required. As $\dim_K(L) = 2$ this means that $\{1, \lambda\}$ is a basis for L over K.

We can therefore write $-\lambda^2$ in terms of this basis, say as $-\lambda^2 = b\lambda + c$, or equivalently $\lambda^2 + b\lambda + c = 0$. Next put $\alpha = \lambda + b/2 \in L$. We find that $\alpha^2 = \lambda^2 + b\lambda + b^2/4 = -c + b^2/4 \in K$. By the same logic as for λ we also see that $\{1, \alpha\}$ is a basis for L and so $L = K(\alpha)$, which proves (a).

Now suppose we have another element $\beta \in L \setminus K$ with $\beta^2 \in K$. We can write $\beta = x + y\alpha$ for some $x, y \in K$. As $\beta \notin K$ we have $y \neq 0$. This gives

$$\beta^2 = (x^2 + y^2 a) + 2xy\alpha,$$

which is assumed to lie in K, so we must have $2xy = 0$. As $y \neq 0$ this gives $x = 0$ and thus $\beta = y\alpha$, proving (b).

Next, as $\{1, \alpha\}$ is a basis, we can define a K-linear map $\sigma\colon L \to L$ by

$$\sigma(x + y\alpha) = x - y\alpha,$$

for any $x, y \in K$. This satisfies $\sigma(\sigma(x + y\alpha)) = \sigma(x - y\alpha) = x + y\alpha$, so $\sigma^2 = \mathrm{id}$. It also has $\sigma(0) = 0$ and $\sigma(1) = 1$. Now consider elements $\mu = u + v\alpha$ and $\nu = x + y\alpha$ in L. We have

$$\begin{aligned}
\mu\nu &= (ux + vya) + (vx + uy)\alpha, \\
\sigma(\mu\nu) &= (ux + vya) - (vx + uy)\alpha, \\
\sigma(\mu)\sigma(\nu) &= (u - v\alpha)(x - y\alpha) = (ux + vya) - (vx + uy)\alpha = \sigma(\mu\nu),
\end{aligned}$$

so σ is a field automorphism.

Now let τ be any other automorphism of L with $\tau|_K = \mathrm{id}$. Write $a = \alpha^2 \in K$. We can apply τ to the equation $\alpha^2 - a = 0$ to get $\tau(\alpha)^2 - a = 0$, or in other words $\tau(\alpha)^2 - \alpha^2 = 0$, or in other words $(\tau(\alpha) - \alpha)(\tau(\alpha) + \alpha) = 0$, so either $\tau(\alpha) = \alpha$ or $\tau(\alpha) = -\alpha$. In the first case we have $\tau = \mathrm{id}$, and in the second case we have $\tau = \sigma$. It follows that $\mathrm{Gal}(L/K) = \{\mathrm{id}, \sigma\}$ as claimed. ⊠

Proposition 10.2 Let p and q be distinct prime numbers, put

$$B = \{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\} \subset \mathbb{R},$$

and let L be the span of B over $\mathbb{Q}$.

(a) The set B is linearly independent over $\mathbb{Q}$, so is a basis for L, and $[L : \mathbb{Q}] = 4$.

(b) L is a splitting field for the polynomial $(t^2 - p)(t^2 - q) \in \mathbb{Q}[t]$.

(c) There are automorphisms σ and τ of L given by

$$\begin{aligned}\sigma(w + x\sqrt{p} + y\sqrt{q} + z\sqrt{pq}) &= w - x\sqrt{p} + y\sqrt{q} - z\sqrt{pq} \\ \tau(w + x\sqrt{p} + y\sqrt{q} + z\sqrt{pq}) &= w + x\sqrt{p} - y\sqrt{q} - z\sqrt{pq}.\end{aligned}$$

(d) We have $\sigma^2 = \tau^2 = 1$ and $\sigma\tau = \tau\sigma$, and $\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \simeq C_2 \times C_2$.

PROOF: For part (a), consider a nontrivial linear relation $w + x\sqrt{p} + y\sqrt{q} + z\sqrt{pq} = 0$. Here $w, x, y, z \in \mathbb{Q}$, but after multiplying through by a suitable integer we can clear the denominators and so assume that $w, x, y, z \in \mathbb{Z}$. We can then divide through by any common factor and thus assume that $\gcd(w, x, y, z) = 1$. Now rearrange the relation as $w + x\sqrt{p} = -(y + z\sqrt{p})\sqrt{q}$ and square both sides to get

$$(w^2 + px^2) + 2wx\sqrt{p} = (y^2 + pz^2)q + 2yzq\sqrt{p}.$$

We know that 1 and $\sqrt{p}$ are linearly independent over $\mathbb{Q}$, so we conclude that

$$\begin{aligned} wx &= yzq, \\ w^2 + px^2 &= (y^2 + pz^2)q. \end{aligned}$$

From the first of these we see that either w or x is divisible by q. In either case we can feed this fact into the second equation to see that w^2 and x^2 are both divisible by q, so w and x are both divisible by q, say $w = qw'$ and $x = qx'$. We can substitute these in the previous equations and cancel common factors to get

$$\begin{aligned} yz &= w'x'q \\ y^2 + pz^2 &= (w'^2 + px'^2)q. \end{aligned}$$

The same logic now tells us that y and z are both divisible by q, contradicting the assumption that $\gcd(w,x,y,z)=1$. It follows that there can be no such linear relation, which proves (a).

For (b), the main point to check is that L is actually a subfield of $\mathbb{R}$. To see this, write $e_0=1$, $e_1=\sqrt{p}$, $e_2=\sqrt{q}$ and $e_3=\sqrt{pq}$. By a straightforward check of the 16 possible cases, we see that e_ie_j is always a rational multiple of e_k for some k (for example $e_1e_3=pe_2$). In particular, we have $e_ie_j\in L$. Now suppose we have two elements $x,y\in L$, say $x=\sum_{i=0}^3 x_ie_i$ and $y=\sum_{j=0}^3 y_je_j$. Then $xy=\sum_{i,j}x_iy_je_ie_j$ with $x_iy_j\in\mathbb{Q}$ and $e_ie_j\in L$, and L is a vector space over $\mathbb{Q}$, so $xy\in L$. We therefore see that L is a subring of $\mathbb{R}$. As L is finite-dimensional it follows that L is a subfield of $\mathbb{R}$. It is clearly generated by the roots of the polynomial

$$f(t)=(t^2-p)(t^2-q)=(t-\sqrt{p})(t+\sqrt{p})(t-\sqrt{q})(t+\sqrt{q}),$$

so it is a splitting field for $f(t)$.

Next, we can regard L as a degree two extension of $\mathbb{Q}(\sqrt{q})$ obtained by adjoining a square root of p. Proposition 10.1 therefore gives us an automorphism σ of L that acts as the identity on $\mathbb{Q}(\sqrt{q})$, and this is clearly described by the formula stated above. Similarly, we obtain the automorphism τ by regarding L as $\mathbb{Q}(\sqrt{p})(\sqrt{q})$ rather than $\mathbb{Q}(\sqrt{q})(\sqrt{p})$. This proves (c).

Now let θ be an arbitrary automorphism of L (which automatically acts as the identity on $\mathbb{Q}$). We must then have $\theta(\sqrt{p})^2=\theta(\sqrt{p}^2)=\theta(p)=p$, so $\theta(\sqrt{p})=\pm\sqrt{p}$. Similarly we have $\theta(\sqrt{q})=\pm\sqrt{q}$, and it follows by inspection that there is a unique automorphism $\varphi\in\{1,\sigma,\tau,\sigma\tau\}$ that has the same effect on $\sqrt{p}$ and $\sqrt{q}$ as θ. This means that the automorphism $\psi=\varphi^{-1}\theta$ has $\psi(\sqrt{p})=\sqrt{p}$ and $\psi(\sqrt{q})=\sqrt{q}$, and therefore also $\psi(\sqrt{pq})=\psi(\sqrt{p})\psi(\sqrt{q})=\sqrt{pq}$. As B is a basis for L over $\mathbb{Q}$ and ψ acts as the identity on B, we see that $\psi=\mathrm{id}$, and so $\theta=\varphi$. This proves (d). $\boxtimes$

We next consider two different cubic equations for which the answers work out quite neatly. In a later section we will see that general cubics are conceptually not too different, although the formulae are typically less tidy.

Example 10.3 We will construct and study a splitting field for the polynomial $f(x)=x^3-3x-3\in\mathbb{Q}[x]$. This is an Eisenstein polynomial for the prime 3, so it is irreducible over $\mathbb{Q}$. We start by noting that $(3+\sqrt{5})/2$ is a positive real number, with inverse $(3-\sqrt{5})/2$. We let β denote the real cube root of $(3+\sqrt{5})/2$, so that β^{-1} is the real cube root of $(3-\sqrt{5})/2$. Then put $\omega=(\sqrt{-3}-1)/2\in\mathbb{C}$, so $\omega^3=1$ and $\omega^2+\omega+1=0$. Finally, put $\alpha_i=\omega^i\beta+1/(\omega^i\beta)$ for $i=0,1,2$.

We claim that these are roots of $f(x)$. Indeed, we have

$$\begin{aligned}\alpha_i^3 &= (\omega^i\beta)^3 + 3(\omega^i\beta)^2/(\omega^i\beta) + 3\omega^i\beta/(\omega^i\beta)^2 + 1/(\omega^i\beta)^3 \\ &= \beta^3 + \beta^{-3} + 3(\omega^i\beta + \omega^{-i}\beta^{-1}) \\ &= (3+\sqrt{5})/2 + (3-\sqrt{5})/2 + 3\alpha_i = 3 + 3\alpha_i,\end{aligned}$$

which rearranges to give $f(\alpha_i) = 0$ as claimed. We also note that α_0 is real, whereas α_1 and α_2 are non-real and are complex conjugates of each other. It follows that we have three distinct roots of $f(x)$, and thus that $f(x) = (x-\alpha_0)(x-\alpha_1)(x-\alpha_2)$, so the splitting field is generated by α_0, α_1 and α_2. We write L for this splitting field.

Next, note that $\overline{\omega}$ (the complex conjugate of ω) is ω^{-1}, and so $\overline{\alpha_1} = \alpha_2$ and $\overline{\alpha_2} = \alpha_1$, whereas $\overline{\alpha_0} = \alpha_0$ because α_0 is real. This means that conjugation permutes the roots α_i and so preserves L. We thus have an automorphism $\sigma\colon L \to L$ given by $\sigma(a) = \overline{a}$ for all $a \in L$.

We also claim that there is an automorphism ρ of L with $\rho(\alpha_0) = \alpha_1$ and $\rho(\alpha_1) = \alpha_2$ and $\rho(\alpha_2) = \alpha_0$. Indeed, Proposition 9.2 tells us that there is an automorphism λ such that $\lambda(\alpha_0) = \alpha_1$. We know that λ permutes the set $R = \{\alpha_0, \alpha_1, \alpha_2\}$ of roots of $f(x)$, so it must either be the three-cycle $(\alpha_0\ \alpha_1\ \alpha_2)$ or the transposition $(\alpha_0\ \alpha_1)$. In the first case, we can just take $\rho = \lambda$; in the second, we can take $\rho = \lambda\sigma$. It is now easy to check that the set $\{1, \rho, \rho^2, \sigma, \rho\sigma, \rho^2\sigma\}$ gives all six permutations of R. It follows that the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is $\S_3$.

Example 10.4 Consider the polynomial $f(x) = x^3 + x^2 - 2x - 1$. We first claim that this is irreducible over $\mathbb{Q}$. Indeed, if it were reducible we would have $f(x) = g(x)h(x)$ for some monic polynomials $g(x), h(x) \in \mathbb{Q}[x]$ with $\deg(g(x)) = 1$ and $\deg(h(x)) = 2$. Gauss' Lemma would then tell us that $g(x), h(x) \in \mathbb{Z}[x]$. This would mean that $g(x) = x - a$ for some $a \in \mathbb{Z}$, and thus $f(a) = 0$. However, we have $f(2m) = 2(4m^3 + 2m^2 - m) - 1$ and $f(2m+1) = 2(4m^3 + 8m^2 + 3m) - 1$ so $f(a)$ is odd for all $a \in \mathbb{Z}$, which is a contradiction.

We now exhibit the roots of $f(x)$. Write

$$\begin{aligned}\zeta &= \exp(2\pi i/7) = \cos(2\pi/7) + i\sin(2\pi/7) \\ \alpha &= \zeta + \zeta^{-1} = 2\cos(2\pi/7) \\ \beta &= \zeta^2 + \zeta^{-2} = 2\cos(4\pi/7) \\ \gamma &= \zeta^4 + \zeta^{-4} = 2\cos(8\pi/7).\end{aligned}$$

(Remember that $\zeta^4 = \zeta^{-3}$.) We claim that α, β and γ are roots of $f(x)$. First calculate $f(\alpha)$. We have:

$$\begin{aligned} \alpha^3 &= \zeta^{-3} + 3\zeta^{-1} + 3\zeta + \zeta^3 \\ \alpha^2 &= \zeta^{-2} + 2 + \zeta^2 \\ -2\alpha &= -2\zeta^{-1} - 2\zeta \\ -1 &= -1. \end{aligned}$$

If we add together the left hand sides we get $f(\alpha)$, and if we add together the right hand sides we get $\sum_{i=-3}^{3} \zeta^i$.

Now remember that $\zeta^7 = 1$ and $\zeta \neq 1$, so

$$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0.$$

Dividing by ζ^3 we get $\sum_{i=-3}^{3} \zeta^i = 0$, so $f(\alpha) = 0$.

By a modification of this calculation we also have $f(\beta) = f(\gamma) = 0$.

We now have three distinct roots for the cubic polynomial $f(x)$, so we have

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma).$$

We now claim that

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta, \gamma). \tag{1}$$

First, observe that

$$\begin{aligned} \alpha^2 - 2 &= (\zeta^{-2} + 2 + \zeta^2) - 2 = \zeta^{-2} + \zeta^2 = \beta \\ \beta^2 - 2 &= (\zeta^{-4} + 2 + \zeta^4) - 2 = \zeta^{-4} + \zeta^4 = \gamma \\ \gamma^2 - 2 &= (\zeta^{-8} + 2 + \zeta^8) - 2 = \zeta^{-8} + \zeta^8 = \zeta^{-1} + \zeta = \alpha. \end{aligned}$$

The first of these shows that $\beta \in Q(\alpha)$, and so $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$. From the other equations we see that $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\beta)$ and $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\gamma)$. Altogether we have $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$, which implies (1).

So $\mathbb{Q}(\alpha)$ is a splitting field for $f(x)$.

Next, Proposition 9.2 tells us that there is an automorphism σ of $\mathbb{Q}(\alpha)$ with $\sigma(\alpha) = \beta$. Applying σ to $\beta = \alpha^2 - 2$ we get

$$\sigma(\beta) = \sigma(\alpha^2 - 2) = \sigma(\alpha)^2 - 2 = \beta^2 - 2 = \gamma.$$

By a similar argument we have $\sigma(\gamma) = \gamma^2 - 2 = \alpha$, so σ corresponds to the three-cycle $(\alpha\ \beta\ \gamma)$. We also know that $|\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, and it follows that $\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma, \sigma^2\} \simeq C_3$.

Example 10.5 Consider the polynomial $f(x) = x^4 - 10x^2 + 20$, which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion at the prime 5. This is a quadratic function of x^2, so by the usual formula it vanishes when $x^2 = (10 \pm \sqrt{100 - 4 \times 20})/2 = 5 \pm \sqrt{5}$ (and both of these values are positive real numbers). The roots of $f(x)$ are therefore α, β, $-\alpha$ and $-\beta$ where $\alpha = \sqrt{5+\sqrt{5}}$ and $\beta = \sqrt{5-\sqrt{5}}$. It is a special feature of this example that β can be expressed in terms of α. To see this, note that $\alpha^2 = 5 + \sqrt{5}$ and so $\alpha^4 = 30 + 10\sqrt{5}$. Then put $\beta' = \frac{1}{2}\alpha^3 - 3\alpha$ and note that

$$\begin{aligned}
\alpha\beta' &= \tfrac{1}{2}\alpha^4 - 3\alpha^2 = 15 + 5\sqrt{5} - 15 - 3\sqrt{5} = -2\sqrt{5} \\
\alpha\beta &= \sqrt{(5+\sqrt{5})(5-\sqrt{5})} = \sqrt{5^2 - \sqrt{5}^2} = \sqrt{25-5} = 2\sqrt{5}.
\end{aligned}$$

This shows that $\alpha\beta' = -\alpha\beta$, so $\beta = -\beta' = -(\frac{1}{2}\alpha^3 - \alpha) \in \mathbb{Q}(\alpha)$. This shows that all roots of $f(x)$ lie in $\mathbb{Q}(\alpha)$, so $\mathbb{Q}(\alpha)$ is a splitting field for $f(x)$ over $\mathbb{Q}$. By Proposition 9.2 there is an automorphism σ of $\mathbb{Q}(\alpha)$ with $\sigma(\alpha) = \beta$. It follows that

$$\sigma(\sqrt{5}) = \sigma(\alpha^2 - 5) = \sigma(\alpha)^2 - 5 = \beta^2 - 5 = -\sqrt{5}.$$

We now apply σ to the equation $\alpha\beta = 2\sqrt{5}$ to get $\beta\sigma(\beta) = -2\sqrt{5}$. We can then divide this by the original equation $\alpha\beta = 2\sqrt{5}$ to get $\sigma(\beta)/\alpha = -1$, so $\sigma(\beta) = -\alpha$. Moreover, as σ is a homomorphism we have $\sigma(-a) = -\sigma(a)$ for all a, so $\sigma(-\alpha) = -\beta$ and $\sigma(-\beta) = \alpha$. This shows that σ corresponds to the four-cycle $(\alpha\ \beta\ -\alpha\ -\beta)$. It follows that the automorphisms $\{1, \sigma, \sigma^2, \sigma^3\}$ are all different, but $|\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, so we have

$$\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3\} \simeq C_4.$$