EXTENSIONS WITH GALOIS GROUP C_3

N. P. STRICKLAND

Fix a rational number q, and note that the number

$$r = q^2 + q + 1 = (q + 1/2)^2 + 3/4$$

is always strictly positive. Consider the polynomial

$$f(x) = x^3 - (3x - 2q - 1)r.$$

Alternatively, this is the most general polynomial of the form

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

with $b \neq 0$ but $a = 9b^2 + 27c^2 + 4b^3 = 0$; the parameter q can be recovered as $q = -(b + 3c)/(2b)$.

Note that the roots of $f'(x)$ are $\pm\sqrt{r}$, and that

$$f(\pm\sqrt{r}) = 2(q + \tfrac{1}{2} \pm \sqrt{r}) = 2\left((q + \tfrac{1}{2}) \pm \sqrt{(q + \tfrac{1}{2})^2 + \tfrac{3}{4}}\right).$$

From this we check that $f(-\sqrt{r}) > 0 > f(+\sqrt{r})$. It follows that there is a unique root α of $f(x)$ with $\alpha < -\sqrt{r}$, and a unique root β with $-\sqrt{r} < \beta < +\sqrt{r}$, and a unique root γ with $+\sqrt{r} < \gamma$. We put $K = \mathbb{Q}(\alpha, \beta, \gamma) \subset \mathbb{R}$, which is a splitting field for $f(x)$ over $\mathbb{Q}$.

Another way to check that there are three distinct roots is to use the identity

$$(2x + 2q + 1)(x\,f'(x) - 3f(x)) - 4r\,f'(x) = 9r,$$

which is a nonzero constant.

Now put $s(x) = x^2 + qx - 2r$. One can check that $f(s(x)) = f(x)g(x)$, where

$$g(x) = x^3 + 3qx^2 - 3(q + 1)x - (4q^3 + 6q^2 + 6q + 1).$$

It follows that s preserves the set $R = \{\alpha, \beta, \gamma\}$ of roots of $f(x)$. One can also check that in $\mathbb{Q}[x]$ we have

$$x + s(x) + s(s(x)) = (x + 2q)f(x),$$

so $\theta + s(\theta) + s(s(\theta)) = 0$ whenever $\theta \in R$. We can compare this equation for θ with the corresponding equation for $s(\theta)$ to see that $s(s(s(\theta))) = \theta$. It follows that s acts on R either as the identity or as a 3-cycle. The first option is incompatible with the equation $\theta + s(\theta) + s(s(\theta)) = 0$ (because at least two of the roots are nonzero). It follows that s acts as a 3-cycle, and thus that $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\gamma)$. In particular, if any one of the roots is rational, then they all are.

From now on we suppose that the roots are all irrational, so $f(x)$ is irreducible and $K \simeq \mathbb{Q}[x]/f(x)$. In this context we see that there is an automorphism σ of K with $\sigma(\theta) = s(\theta)$ for all $\theta \in R$, and that $G(K/\mathbb{Q})$ is cyclic of order 3, generated by σ.

Now put $\omega = (\sqrt{-3} - 1)/2 \in \mathbb{C}$ and $L = \mathbb{Q}(\omega)$ and $M = KL$. The usual theory of cyclic extensions tells us that the element

$$\lambda = \frac{\omega - q}{3r}(\alpha + \omega^2\sigma(\alpha) + \omega\sigma^2(\alpha))$$

satisfies $\lambda^3 \in L$ and $M = L(\lambda)$. In fact, one can check that

$$\lambda^3 = \frac{\omega - q}{\omega^2 - q} = (\omega - q)^2/r.$$

References