Series 12, Bonus Exercise

David Wiedemann

5 juin 2022

1

Recall from a theorem that, to show that $f = x^3 + ax + 1, a \in \mathbb{Z}_+$ is irreducible over $\mathbb{Q}$, it suffices to show that it has no roots over $\mathbb{Q}$. Hence, suppose that $\frac{w}{z} \in \mathbb{Q}$ is a zero of f, further, without loss of generality suppose that w and z share no common factors. Plugging this into f yields

$$\frac{w^3}{z^3} + a\frac{w}{z} + 1 = 0$$
$$w^3 + awz^2 + z^3 = 0$$
$$w^3 = z^2(-aw - z)$$

Thus w and z share at least one common factor, a contradiction.
As such, we conclude that f has no roots over $\mathbb{Q}$ and is thus irreducible.

2

First notice that by elementary analysis results, f always has at least one real root (f is continuous over $\mathbb{R}$ and $\lim_{x\to+\infty} f = +\infty$, $\lim_{x\to-\infty} f = -\infty$).
Hence, let l be this real root.
In this case, note that over $\mathbb{R}$, f splits as

$$f(x) = (x-l)(x^2+bx+c) = x^3 + (b-l)x^2 + (c-bl)x - lc = x^3 + ax + 1$$

We pretend that in this case, $x^2 + bx + c$ has no real roots, to show this, it is sufficient to show that the discrimant $b^2 - 4c < 0$ As the family $\{x^i\}_{i=0}^{\infty}$ is a basis for the vector space $\mathbb{R}[x]$, we conclude that l, b and c must satisfy the following three equations

$$\begin{cases} b - l = 0 \\ c - bl = a \\ -lc = 1 \end{cases}$$

In particular, $l = b$ and thus $c = a + b^2$.
Then, the discrimant becomes

$$\Delta = b^2 - 4c = b^2 - 4b^2 - 4a = -3b^2 - 4a$$

Now as $a > 0$ and $b^2 > 0$ (as $b \in \mathbb{R}$) ,we conclude that $\Delta < 0$ and thus f does not have three real roots.

3

First, we show that K is indeed of degree 3, ie. that $[K : \mathbb{Q}] = 3$, this follows immediatly from lemma 4.2.25 in the course, indeed, f is irreducible of degree 3 over $\mathbb{Q}$ by part 1 and thus the hypothesis of the proposition applies.

Now we show that K is not Galois over $\mathbb{Q}$, to do this, we construct an embedding of $K \hookrightarrow \mathbb{R}$.
Let $l \in \mathbb{R} \setminus \mathbb{Q}$ be the (unique) real root of f, using a theorem from the course we know that $K \simeq \mathbb{Q}(l)$.
Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, as $\sigma(l)$ must still be a root of f.
As l is the unique root of f in K (as $K \subset \mathbb{R}$ and f has a unique real root) , $\sigma(l) = l$.
As l generates K over $\mathbb{Q}$, this implies that $\sigma = \mathrm{Id}$ and thus $|\mathrm{Gal}(L/\mathbb{Q})| = 1$.
Since an extension $K/\mathbb{Q}$ is Galois iff $[K : \mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})|$, we deduce that K is not Galois over $\mathbb{Q}$.

4

Let l, c_1, c_2 be the three distinct roots of f (where l is the real root and c_1, c_2 are the two complex ones).
By definition, L being the splitting field, it is generated by l, c_1, c_2, ie. $L = \mathbb{Q}(l, c_1, c_2)$.
Using proposition 4.6.3.2 from the course notes, we thus conclude that there exists an injective group morphism $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow S_3$.
Notice that $|S_3| = 3! = 6$ and thus it suffices to show $|\mathrm{Gal}(L/\mathbb{Q})| = 6$, as an injective map between finite sets of same cardinality is bijective.

To show this, first notice that as we are working in characteristic 0, any extension of $\mathbb{Q}$ is separable, this follows from our characterisation of perfect fields.
As L is a splitting field and is generated by separable elements, proposition 4.6.3.4 in fact implies that $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}]$, so we reduce to showing that $[L : \mathbb{Q}] = 6$.
We claim that $[L : K] = 2$.
To show this, notice that as $K = \mathbb{Q}(l)$, $L = K(c_1, c_2)$.

We pretend that $K(c_1) = L$.
Indeed, notice that over K, f splits as $(x-l)(x^2+bx+c), b, c \in K$, as x^2+bx+c is a degree 2 polynomial over K which does not have roots over K, it is irreducible and thus is a minimal polynomial for c_1 (as c_1 obviously is not a root of $x-l$).
From our general quadratic formula, we know that (up to switching the signs in front of the square root) $c_1 = \frac{1}{2}(-b+\sqrt{b^2-4c})$ and $c_2 = \frac{1}{2}(-b-\sqrt{b^2-4c})$, in particular $c_2 = -b - c_1$.
Thus, $K(c_1) \supset K(c_1, c_2)$, as the inclusion $K(c_1) \subset K(c_1, c_2)$ is trivial, we deduce that $K(c_1) = L$.
As, $K(c_1) = {}^{K[x]}\!\big/_{(x^2+bx+c)}$, $[K(c_1) : K] = 2$.
As such, we may compute $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 2 \cdot 3 = 6$.
Thus, the injective homomorphism $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow S_3$ is in fact a bijection and thus $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$.