D-MATH
Prof. Brent Doran

Algebra II

FS 2014

Exercise sheet 11

Galois groups

1. Show that the polynomials $(x^2 - 2x - 2)(x^2 + 1)$ and $x^5 - 3x^3 + x^2 - 3$ have the same splitting field over $\mathbb{Q}$. What is the degree of the field extension ?

   Solution : The polynomial

   $$(x^2 - 2x - 2)(x^2 + 1) = (x - (1 + \sqrt{3}))(x - (1 - \sqrt{3}))(x - i)(x + i)$$

   has splitting field $\mathbb{Q}(\sqrt{3}, i)$, while

   $$\begin{aligned} x^5 - 3x^3 + x^2 - 3 &= (x^3 + 1)(x^2 - 3) \\ &= (x + 1)\left(x - \frac{1}{2}(-1 + \sqrt{3}i)\right)\left(x - \frac{1}{2}(-1 - \sqrt{3}i)\right)(x - \sqrt{3})(x + \sqrt{3}) \end{aligned}$$

   has splitting field $\mathbb{Q}(\sqrt{3}, \frac{1}{2}(-1 + \sqrt{3}i))$. We show that the two splitting fields coincide. In fact, one can write

   $$i = \frac{\sqrt{3}}{3}\left(2\left(\frac{1}{2}(-1 + \sqrt{3}i)\right) + 1\right).$$

   Because $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})] = 2$, by the multiplicative property of the degree,

   $$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4.$$

2. Let F be a field. Show that the field extension $F(x)/F$ admits a F-endomorphism of $F(x)$ that is *not* an automorphism.

   Solution : Let φ be the endomorphism of $F(x)$ that is constant on elements of F and sends x to x^2. Then φ is not an automorphism. In fact, we show that x is not contained in the image of φ. Introduce the degree map

   $$d : F(x) \to \mathbb{Z}, \quad d\left(\frac{g(x)}{h(x)}\right) = (\deg(g) - \deg(h)).$$

   Then by direct computation, one can see that for any $f(x) \in F(x)$,

   $$d(\varphi(f)) = 2d(f).$$

   In particular, x is not in the image of φ.

3. Let $f(x)$ be an irreducible polynomial over a field F and denote by K its splitting field. Prove that if the Galois group $G = \mathrm{Gal}(K/F)$ is abelian, then $K = F(\alpha)$ for any root α of $f(x)$.

   Solution : Let α and β be two roots of f. We will show that $F(\alpha) = F(\beta)$ and hence $F(\alpha)$ contains all roots of f and is the splitting field K.

   Consider the subgroups $G_\alpha = \mathrm{Gal}(K/F(\alpha))$ and $G_\beta = \mathrm{Gal}(K/F(\beta))$ of G. There exists $\sigma \in G$ such that $\sigma(\alpha) = \beta$, hence $\sigma(F(\alpha)) = F(\beta)$. Therefore $\sigma G_\alpha \sigma^{-1} = G_\beta$.

   By assumption, G is abelian. Hence, because $\sigma G_\alpha \sigma^{-1} = G_\beta$, we can conclude that $G_\alpha = G_\beta$ and $F(\alpha) = F(\beta)$.

4. Exhibit a polynomial $f(x) \in \mathbb{Q}[x]$ of even degree $n \geqslant 2$ with Galois group $\mathbb{Z}/(2)$.

   Solution : Consider $\prod_{k \leqslant n}(x^2 + k^2)$. Its splitting field is $\mathbb{Q}(i)$. There are only two $\mathbb{Q}$-automorphisms of $\mathbb{Q}(i)$, namely the identity and complex conjugation. Hence the Galois group is $\mathbb{Z}/(2)$.

5. Consider the group

$$H = \left\{ \sigma_a : a \in \mathbb{C},\ \sigma_a \left(\frac{g(x)}{h(x)} \right) = \frac{g(x+a)}{h(x+a)} \right\}$$

   of $\mathbb{C}$-automorphisms of the field $\mathbb{C}(t)$ of rational functions. Show that $\mathbb{C}(t)^H = \mathbb{C}$.

   Solution : Let us assume that g and h are relatively prime. Setting

$$\frac{g(x)}{h(x)} = \frac{g(x+a)}{h(x+a)}$$

   it follows $g(x)$ divides $g(x+a)$. Comparing the term of highest degree in $g(x+a) = \lambda g(x)$, we conclude that $\lambda = 1$. If $a \neq 0$ and g is not a constant polynomial, this is not possible.