Solutions of exercise sheet 4

1. Let K be a field of characteristic 2, and fix an algebraic closure $\bar{K}$ of K. Suppose L/K is a Galois quadratic extension contained in $\bar{K}$.

1. Show that there exists $a \in K$ such that $L = K(b)$ where b is a root of $X^2 - X + a$.
2. Prove that $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$, and express the action of the generator of G on L as a matrix with respect to the basis $(1, b)$.
3. Suppose that for $i = 1, 2$ we have elements $a_i \in K$ and we consider the field extensions $L_i = K(b_i)$, where $b_i \in \bar{K}$ are roots of polynomials $X^2 - X + a_i$, which we suppose to be irreducible. Show that $L_1 = L_2$ if and only if there exists $\mu \in K$ such that $\mu^2 - \mu = a_2 - a_1$.

Solution:

1. Let $b_0 \in L \setminus K$ and $f(X) = X^2 - sX + t$ its minimal polynomial over K. Let us first notice that $s \neq 0$. Else, we would have $b_0^2 = -t$, giving
$$f(X) = X^2 + t = (X - b_0)(X + b_0) = (X - b_0)^2$$
since $\mathrm{char}(L) = \mathrm{char}(K) = 2$, so that f would not be separable and L/K would not be Galois, contradiction.
Now b_0 necessarily generates the whole L, and in order to find an element b in $L = K(b_0)$ giving a minimal polynomial of the form $X^2 - X + a$, we write $b = \lambda b_0 + \mu$ for $\lambda, \mu \in K$ and require $b^2 - b \in K$. This gives (using the fact that the characteristic is 2):
$$K \ni \lambda^2 b_0^2 + \mu^2 - \lambda b_0 - \mu = \lambda^2(sb_0 - t) + \mu^2 - \lambda b_0 - \mu,$$
which by K-linear independence of 1 and b_0 is equivalent to $\lambda^2 s - \lambda = 0$. This is true if and only if $\lambda = 0$ or $\lambda = \frac{1}{s}$. The first possibility is not good because then b would lie in K. So it is enough to choose $b = x/s$ in order to obtain $b^2 - b + \frac{t}{s^2} = 0$, meaning that b is a root of the polynomial $g(X) = X^2 - X + a$ for $a = t/s^2$ and $L = K(b)$.
2. Since $\mathrm{Gal}(L/K) = [L : K] = 2$, the only possibility is that we have a cyclic Galois group of order 2. It is generated by the non-trivial K-automorphism τ of L, which sends b to another root of g. But it is clear that $b + 1$ is also a root of $g(X)$, so that $\tau(1) = 1$, $\tau(b) = 1 + b$, and
$$[\tau]_{\{1,b\}} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

3. First, notice that L_1 and L_2 are both quadratic extensions of K, so that they coincide if and only if $L_1 \subseteq L_2$, if and only if $b_1 = \lambda b_2 + \mu$ for some $\lambda, \mu \in K$. This condition is equivalent (eventually by translating μ by 1) to saying that there are $\lambda, \mu \in K$ such that $\lambda b_2 + \mu$ is a root of $X^2 - X + a_1$. This in turns is equivalent to saying that for some $\lambda, \mu \in K$ we have

$$0 = \lambda^2 b_2^2 + \mu^2 - \lambda b_2 - \mu + a_1 = \lambda^2 (b_2 - a_2) - \lambda b_2 + \mu^2 - \mu + a_1,$$

where the second equality comes from the hypothesis on b_2. By linear independence of 1 and b_2 we see that $\lambda^2 = \lambda$, and the only possibility (as $b_1 \notin K$) is that $\lambda = 1$.

This means that $L_1 = L_2$ if and only there exists $\mu \in K$ such that $\mu^2 - \mu = a_2 - a_1$, as desired.

2. Consider the polynomial $f = X^3 - 2 \in \mathbb{Q}[X]$, and let L be the splitting field of f.

1. Prove that $[L : \mathbb{Q}] = 6$, and find intermediate extensions L_1 and L_2 of L over $\mathbb{Q}$ such that $[L_1 : \mathbb{Q}] = 2$ and $[L_2 : \mathbb{Q}] = 3$.
2. Prove that $L/\mathbb{Q}$ is a Galois extension with Galois group $G = S_3$ [*Hint:* The Galois group of L acts faithfully on the roots of f].
3. Which of the four field extensions L/L_i and $L_i/\mathbb{Q}$, for $i = 1, 2$ are Galois? Find their Galois groups.

Solution:

1. Let ξ be a primitive third root of unity. Then we have a decomposition

$$f(X) = (X - \sqrt[3]{2})(X - \xi \sqrt[3]{2})(X - \xi^2 \sqrt[3]{2}),$$

so that $L = \mathbb{Q}(\sqrt[3]{2}, \xi)$. We have that $L_2 := \mathbb{Q}(\sqrt[3]{2})$ is an intermediate field extension of L with degree 3 over $\mathbb{Q}$. Moreover, $\xi \notin \mathbb{R} \supseteq L_2$, so that L/L_2 is non-trivial. Notice that ξ satisfies the cyclotomic polynomial $X^2 + X + 1 \in \mathbb{Q}[X] \subseteq L_2[X]$, so that $[L : L_2] = 2$ necessarily. This implies that $[L : \mathbb{Q}] = 6$. We can also consider $L_1 := \mathbb{Q}(\xi)$ to get an intermediate field extension of degree 2 over $\mathbb{Q}$ as required.

2. The Galois group G acts faithfully on the 3 roots of f, so that $G \subseteq S_3$. But $|G| = [L : \mathbb{Q}] = 6 = |S_3|$, so that we need $G = S_3$.
3. The only non-Galois extension is $L_2/\mathbb{Q}$, because the minimal polynomial of $\sqrt[3]{2}$ does not split in $L_2[X]$. For the other extensions, separability is always clear, and normality is immediate for $L_1/\mathbb{Q}$ and L/L_2 which have degree 2, while L/L_1 is normal because there the minimal polynomial of $\sqrt[3]{2}$ splits completely, and $L = L_1(\sqrt[3]{2})$ by construction.

   Since all groups of cardinality 2 and 3 are cyclic, we have $\mathrm{Gal}(L/L_2) \cong \mathrm{Gal}(L_1/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Gal}(L/L_1) \cong \mathbb{Z}/3\mathbb{Z}$. Notice that indeed we have $\mathrm{Aut}_{\mathbb{Q}}(L_2) = \{\mathrm{id}\}$.

See next page!

3. Let K be a field and $P \in K[X]$ a separable degree-n irreducible polynomial, L its splitting field and $G = \mathrm{Gal}(L/K)$.

0. Prove that $|G| \leq \deg(P)!$

From now on, assume that P is a palindromic monic polynomial of even degree, i.e., there exist a positive integer d and elements $a_1, \ldots, a_d$ such that

$$P = X^{2d} + a_1 X^{2d-1} + \cdots + a_{d-1}X^{d+1} + a_d X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + 1.$$

Show that:

1. The set of roots Z_P of P is stable under $x \mapsto \frac{1}{x}$.
2. Given the following subgroup of $S_{2d} = \mathrm{Sym}(\{\alpha_1^+, \alpha_1^-, \alpha_2^+, \alpha_2^-, \ldots, \alpha_d^+, \alpha_d^-\})$:

$$W_{2,d} = \{\sigma \in S_{2d} | \, \forall i \, \exists j : \sigma(\{\alpha_i^+, \alpha_i^-\}) = \{\alpha_j^+, \alpha_j^-\}\},$$

   we have that G can be embedded in $W_{2,d}$.
3. $|G| \leq 2^d d!$

Solution:

0. As seen in class, G acts faithfully on the roots of P. This means that we have an injection $G \hookrightarrow \mathrm{Sym}(Z_P)$, where Z_P denotes the set of roots of P, which has cardinality $\deg(P)$ by separability of P. Then $|G| \leq |\mathrm{Sym}(Z_P)| = \deg(P)!$ as desired.
1. One can write $P(X) = a_d X^d + \sum_{i=0}^{d-1} a_i (X^{2d-i} + X^i)$, with $a_0 := 1$. Suppose that $x \in Z_P$. Then $P(x) = 0$, and

$$P\left(\frac{1}{x}\right) = a_d x^{-d} + \sum_{i=0}^{d-1} a_i (x^{-(2d-i)} + x^{-i}) = \frac{1}{x^{2d}} \left(a_d x^{-d} + \sum_{i=0}^{d} a_i (x^i + x^{2d-i}) \right)$$
$$= \frac{1}{x^{2d}} P(x) = 0,$$

   so that Z_P is stable under $x \mapsto \frac{1}{x}$.
2. Notice that the inversion map $L^\times \longrightarrow L^\times$ sending $x \mapsto 1/x$ is an involution (it is its own inverse) and has only two fixed points ± 1. By irreducibility of P, $K \ni \pm 1 \notin Z_P$, so that $Z_p = \{x_1, x_1^{-1}, \ldots, x_d, x_d^{-1}\}$ for some $x_i \in L$ with $x_i \neq x_j^{\pm 1}$ for $i \neq j$. Then the image of G via the embedding $G \hookrightarrow S_{2d}$ from part 1 has to lie inside $W_{2,d}$ (here we identify α_i^* with x_i^{*1} for each $i = 1, \ldots, d$ and sign $* \in \{+, -\}$), because $\sigma(x_i^{-1}) = \sigma(x_i)^{-1}$ for each i.
3. This just amounts to checking that $|W_{2,d}| = 2^d d!$. Since $W_{2,d}$ consists of permutations and the sets of two elements $A_i = \{a_i^+, a_i^-\}$ are pairwise disjoint for $i = 1, \ldots, d$, we have that each $\sigma \in W_{2,d}$ defines a unique permutation $\tau_\sigma \in S_d$ such that $\tau_\sigma(i) = j$ if and only if $\sigma(A_i) = A_j$. Moreover, σ defines a d-tuple of

Please turn over!

signs $(\varepsilon_{\sigma,i})$, where $\varepsilon_{\sigma,i}$ is the sign of $\sigma(a_i^+)$. It is easily seen that σ can be uniquely recovered from τ_σ and the $\sigma(a_i^+)$ as $\sigma(a_i^\varepsilon) = a_{\tau_\sigma(i)}^{\varepsilon\cdot\varepsilon_{\sigma,i}}$. In other words, we have just defined a bijection

$$W_{2,d} \xrightarrow{\sim} S_d \times \{\pm 1\}^d,$$

and we get $|W_{2,d}| = |S_d \times \{\pm1\}^d| = |S_d| \cdot |\{\pm1\}|^d = d!2^d$ as desired.

4. Let $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

1. Show that K is Galois over $\mathbb{Q}$ with Galois group the $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
2. Now let $L = K\left[\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}\right]$. Show that L is Galois over $\mathbb{Q}$.

Solution:

1. Viewing K as $\mathbb{Q}(\sqrt{3})[X]/(X^2-2)$ (resp., as $\mathbb{Q}(\sqrt{2})[X]/(X^2-3)$), we see that $\sqrt{2} \mapsto \pm\sqrt{2}$ (resp., $\sqrt{3} \mapsto \pm\sqrt{3}$) define automorphisms of K over $\mathbb{Q}(\sqrt{3})$ (resp., over $\mathbb{Q}(\sqrt{2})$), and in particular over $\mathbb{Q}$. Hance $\mathrm{Aut}_{\mathbb{Q}}(K)$ contains the identity, σ_2 (which fixes $\sqrt{3}$ and changes sign to $\sqrt{2}$) and σ_3 (which fixes $\sqrt{2}$ and changes sign to $\sqrt{3}$). Clearly, $\sigma_2 \circ \sigma_3$ is none of the previous $\mathbb{Q}$-automorphisms of K, so that $4 \le |\mathrm{Aut}_{\mathbb{Q}}(K)| \le [K:\mathbb{Q}] = 4$ (see Exercise 4 from Exercise sheet 1), meaning that $|\mathrm{Aut}_{\mathbb{Q}}(K)| = 4$ and $K/\mathbb{Q}$ is a Galois extension by Exercise 3 of Exercise sheet 3. In particular, we easily see that $\sigma_2^2 = \sigma_3^2 = (\sigma_2\sigma_3)^2 = \mathrm{id}$, so that $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
2. Let $x = \sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}$. We will prove that $L = K[x]/\mathbb{Q}$ is Galois by checking that x has a separable minimal polynomial over $\mathbb{Q}$ which splits completely in L.
First, let us check that $x \notin K$, so that $[L:K] = 2$ and $[L:\mathbb{Q}] = 8$. This amounts to proving that $x^2 = (\sqrt{2}+2)(\sqrt{3}+3)$ is not a square in K, and can of course be checked directly by imposing an equality $(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})^2 = (\sqrt{2}+2)(\sqrt{3}+3)$ with $a,b,c,d \in \mathbb{Q}$ and finding a contradiction. Anyway, we can avoid some computations by considering the map $N^K_{\mathbb{Q}(\sqrt{2})} : K \longrightarrow \mathbb{Q}(\sqrt{2})$ sending $y \mapsto y \cdot \sigma_3(y)$ (it is a *norm* map). It is clearly a multiplicative map, so that it sends squares to squares. In particular, we have that

$$N^K_{\mathbb{Q}(\sqrt{2})}(x^2) = (\sqrt{2}+2)(\sqrt{3}+3)(\sqrt{2}+2)(\sqrt{3}-3) = 2\cdot 3\cdot(\sqrt{2}+2)^2$$

is not a square in $\mathbb{Q}(\sqrt{2})$ since $2\cdot(\sqrt{2}+2)^2$ is but 3 is not. Then $(\sqrt{2}+2)(\sqrt{3}+3)$ itself cannot be a square in K.
For $\varepsilon, \delta \in \{\pm1\}$, let $x_{\varepsilon,\delta} := \sqrt{(\varepsilon\sqrt{2}+2)(\delta\sqrt{3}+3)}$. Then we claim that

$$f(X) := \prod_{\varepsilon,\delta,\gamma\in\{\pm1\}} (X - \gamma x_{\varepsilon,\delta}) \in \mathbb{Q}[X].$$

This holds because

$$f(X) = \prod_{\varepsilon,\delta\in\{\pm1\}} (X^2 - x_{\varepsilon,\delta}^2) \in K,$$

See next page!

and the action of $\mathrm{Gal}(K,\mathbb{Q})$ permutes the $x_{\varepsilon,\delta}$, so that $f(X) \in K^{\mathrm{Gal}(K,\mathbb{Q})}[X] = \mathbb{Q}[X]$.by Galois correspondence.

This implies that f is the minimal polynomial of x (since $[L:\mathbb{Q}] = 8 = \deg(f)$ and $x = x_{1,1}$ is easily seen to be such that $L = \mathbb{Q}(x)$). Then comparing the squares of two roots and using $\mathbb{Q}$-linear independence of $1, \sqrt{2}, \sqrt{3}$ and $\sqrt{6}$ we immediately see that the roots are distinct, proving separability of f. To conclude, we need to check that $\gamma x_{\varepsilon,\delta} \in K(x)$ for each $\varepsilon, \delta, \gamma \in \{\pm 1\}$. The sign γ is not important (as opposites always exist in a field), and clearly $x_{1,1} = x \in K(x)$. Of course $x_{\varepsilon,\delta} \in K(x)$ whenever $x x_{\varepsilon,\delta} \in K$, and this holds in all the remaining cases. Indeed, we have

$$\begin{aligned} x x_{1,-1} &= (-\sqrt{2}+2)\sqrt{-3+9} = (-\sqrt{2}+2)\sqrt{6} \in K, \\ x x_{-1,1} &= (-\sqrt{3}+3)\sqrt{-2+4} = (-\sqrt{3}+3)\sqrt{2} \in K, \end{aligned}$$

and

$$x x_{-1,-1} = \sqrt{(-2+4)(-3+9)} = \sqrt{12} = 2\sqrt{3} \in K.$$

5. Let L/K be a finite Galois extension. Take $x \in L$ and assume that the elements $\sigma(x)$ are all distinct for $\sigma \in \mathrm{Gal}(L/K)$. Show: $L = K(x)$.

Solution:

This is a straightforward application of the Galois correspondence. We have that $K \subseteq K(x) \subseteq L$, so that $K(x)$ corresponds to the subgroup $H_x \leq G := \mathrm{Gal}(L/K)$ consisting of those $\sigma \in G$ fixing the whole $K(x)$. Such a σ would then fix x, and by hypothesis only Id_L does. Then $K(x) = L^{H_x} = L^{\{\mathrm{Id}_L\}} = L$ and we are done.

Another proof: notice that the minimal polynomial f of x over K needs to have degree equal to $|\mathrm{Gal}(L/K)|$, because applying the automorphisms of $\mathrm{Gal}(L/K)$ we obtain $|\mathrm{Gal}(L/K)|$ distinct roots of f by hypothesis. Then $[K(x):K] = |\mathrm{Gal}(L/K)| = [L:K]$ implying $K(x) = L$.