Prof. Dr. Özlem Imamoglu

Solutions Exercise sheet 9

1. (a) Let p be a prime and $f \in \mathbb{Q}[x]$ an irreducible polynomial of degree p with splitting field L. Assume that f has exactly $p-2$ real roots. Show that $\mathrm{Gal}(L:\mathbb{Q}) \simeq S_p$.

Hint: Make use of the following two facts from the theory of finite groups.

i. (Cauchy) If G is a finite group and p is a prime with $p \mid |G|$ then G contains an element of order p.

ii. A $p-$cycle $(a_1, a_2 \cdots a_n)$ with $\{a_1, \ldots a_n\} = \{1, 2, \ldots, n\}$ and a transposition (a_i, a_j) where generate the group S_p.

(b) Show that the Galois group of $x^5 - 4x + 2 \in \mathbb{Q}[x]$ is isomorphic to S_5

Solution:

(a) Let $\mathbb{Q} \subset L \subset \mathbb{C}$ be a splitting field and $\{\alpha_a, \ldots, \alpha_n\} \subset L$ be the roots of f numbered so that $\{\alpha_3, \ldots, \alpha_n\} \subset \mathbb{R}$ We view $G := \mathrm{Gal}(L:\mathbb{Q})$ as a subgroup of S_p.

Let $\sigma : \mathbb{C} \to \mathbb{C}$, be the complex conjugation map where $\sigma(z) = \bar{z}$. Then σ fixes each of the real roots $\alpha_3, \ldots, \alpha_n$ and interchanges α_1 and α_2. Since $L = \mathbb{Q}(\alpha_1, \ldots \alpha_n)$, $\sigma(L) = L$ and $\sigma|_L \in \mathrm{Gal}(L:\mathbb{Q}) < S_p$ is the transposition (12), interchanging the first two roots fixing the others. Since f is irreducible of degree p using Serie 7, question 1 we have that $p \mid |G|$. Using (i), Cauchy's theorem, G contains an element of order p, hence a p cycle φ. Since p is prime, using (ii) we see that σ and φ then generates S_p.

(b) Using Eisenstein criteria we see that $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ is irreducible. Computing the local extrema we see that f has a local minimum at $(4/5)^{1/4}$, a local maximum at $-(4/5)^{1/4}$ and that it has exactly $3 = 5 - 2$ real zeroes. Applting the first part of the question we have that the Galois group is S_5.

2. Let $L : K$ be a finite separable extention. Use Galois theory to show that there are finitely many intermediate fields between L and K. Use Question 1 of Serie 6 to conclude that $L : K$ is simple.

Solution:

Suppose $a_1, \ldots a_n$ generate L over K. Let $g = m_{a_1} \ldots m_{a_n}$, where $m_{a_i} \in K[x]$ is the minimal polynomial of a_i over K. Then g is separable over K. Let $N : K$ be a splitting field of g over K. Since g is separable $N : K$ is a Galois extention. Since $N : K$ is a finite Galois extention, its Galois group G is a finite group of size $[N : K]$ and hence has finitely many subgroups. By the fundamental theorem these subgroups are in a one to one correspondence between intermediate fields between N and K. Since there are finitely many intermediate fields between N and K there are also finitely many intermediate fields between L and K.

3. Determine the Galois group of $x^6 - 8$ over $\mathbb{Q}$.

Solution: We can factor the polynomial above as

$$x^6 - 8 = (x^2 - 2)(x^4 + 2x^2 + 4).$$

The polynomial $x^4 + 2x^2 + 4$ has the four zeros $\pm\sqrt{-1 \pm i\sqrt{3}}$:

$$x^4+2x^2+4 = \left(x - \sqrt{-1 + i\sqrt{3}}\right)\left(x + \sqrt{-1 + i\sqrt{3}}\right)\left(x - \sqrt{-1 - i\sqrt{3}}\right)\left(x + \sqrt{-1 - i\sqrt{3}}\right)$$

Considering products of pairs of linear terms above, we obtain that there is no polynomial of degree 2 over $\mathbb{Q}$ dividing $x^4 + 2x^2 + 4$. Hence we obtain that the polynomial is irreducible over $\mathbb{Q}$.

Let K be the splitting field of $x^4 + 2x^2 + 4$ over $\mathbb{Q}$.

Now consider the polynomial $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. Since

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

we have $\sqrt{-1 + i\sqrt{3}} + \sqrt{-1 - i\sqrt{3}} = \sqrt{2}$, so $\sqrt{2} \in K$. Hence the splitting field of $x^6 - 8$ over $\mathbb{Q}$ is K. Thus the order $|G| = |\operatorname{Gal}(K : \mathbb{Q})| = 4$.

Hence the Galois group G is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, as those are the only groups of order 4.

Claim. $K = \mathbb{Q}(i\sqrt{6}, \sqrt{2})$.

We have already seen that $\sqrt{-1 + i\sqrt{3}} + \sqrt{-1 - i\sqrt{3}} = \sqrt{2}$. From

$$\left(\sqrt{-1 + i\sqrt{3}} - \sqrt{-1 - i\sqrt{3}}\right)^2 = -1 - 2\sqrt{(-1 + i\sqrt{3})(-1 - i\sqrt{3})} - 1 = -6,$$

we obtain $\mathbb{Q}(i\sqrt{6}, \sqrt{2}) \subseteq K$.

To prove the other inclusion, we will consider the degree of $\mathbb{Q}(i\sqrt{6}, \sqrt{2})$ over $\mathbb{Q}$. Since $i\sqrt{6} \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ and $i\sqrt{6}$ has minimal polynomial $x^2 + 6$ over $\mathbb{Q}(\sqrt{2})$, we have

$$[\mathbb{Q}(i\sqrt{6}, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i\sqrt{6}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4.$$

Hence $\mathbb{Q}(i\sqrt{6}, \sqrt{2}) = K$.

Since $|\operatorname{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})| = 2$ and $|\operatorname{Gal}(\mathbb{Q}(i\sqrt{6}) : \mathbb{Q})| = 2$, we have $\operatorname{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) \cong \operatorname{Gal}(\mathbb{Q}(i\sqrt{6}) : \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. But since $\mathbb{Q}(i\sqrt{6}) \neq \mathbb{Q}(\sqrt{2})$, the Galois group G has 2 *different* subgroups of order 2. Since the group $\mathbb{Z}/4\mathbb{Z}$ only has precisely one subgroup of order 2, G can not be isomorphic to the group $\mathbb{Z}/4\mathbb{Z}$. Since the only other group of order 4 is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we have $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

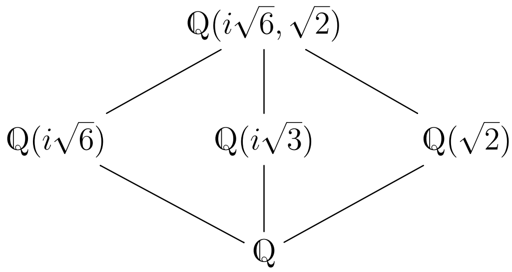
Since the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has 3 different subgroups of order 2, by the Galois correspondence there exists another intermediate field different from $\mathbb{Q}(i\sqrt{6})$ and $\mathbb{Q}(\sqrt{2})$.

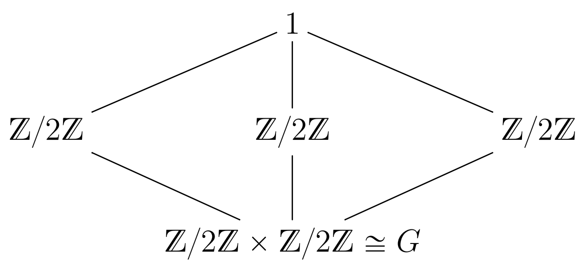
Claim. $i\sqrt{3} \notin \mathbb{Q}(i\sqrt{6})$.

To prove the claim, assume on the contrary that there exist $a_1, a_2, b_1, b_2 \in \mathbb{Q}$, where not both b_1 and b_2 are zero, with

$$\frac{a_1 + a_2 i\sqrt{6}}{b_1 + b_2 i\sqrt{6}} = i\sqrt{3}.$$

But this is equivalent to $a_1 + 3b_2\sqrt{2} = b_1 i\sqrt{3} - a_2 i\sqrt{6}$, which only holds if $a_1 = -3b_2\sqrt{2}$ and $a_2\sqrt{2} = b_1$. But these equations have no solution in $\mathbb{Q}$. Hence $\mathbb{Q}(i\sqrt{6}) \cap \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}$, and since $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, we obtain the following tower of fields corresponding to the groups via the Galois correspondence





4. Let $f(X) \in \mathbb{Q}[X]$ be a non zero polynomial. Assume that the order of the Galois group of $f(x)$ over $\mathbb{Q}$ is odd. Prove that all zeros of $f(x)$ are real.

Solution: Let K be the splitting field of f over $\mathbb{Q}$ and write $G := \mathrm{Gal}(K : \mathbb{Q})$. Note that complex conjugation φ is an automorphism which is always contained in the Galois group G. We also have that $\varphi^2 = \mathrm{id}$, and if f has at least one complex root, the splitting field K would have complex elements and we would have $\mathrm{ord}(\varphi) = 2$. Then 2 would divide the order $|G|$. Hence if the order of the Galois group is odd, complex conjugaion has to have order one, so all roots are real.

5. Let $L : K$ be a finite Galois extension with intermediate fields K_1, K_2 and corresponding Galois groups $G_i := \mathrm{Gal}(L : K_i) \leqslant G := \mathrm{Gal}(L : K)$. Prove:

(a) $K_1K_2 = L^{G_1 \cap G_2}$

(b) $K_1 \cap K_2 = L^{\langle G_1, G_2 \rangle}$, where $\langle G_1, G_2 \rangle$ is the subgroup of G generated by G_1 and G_2

(c) If $K_1K_2 = L$, $K_1 \cap K_2 = K$ and the extensions $K_1 : K$ and $K_2 : K$ are both Galois, then
$$\mathrm{Gal}(L : K) \cong G_1 \times G_2$$
Hint: If G is a group with two normal subgroups G_1 and G_2 such that $G_1 \cap G_2 = 1$, then $G_1G_2 \cong G_1 \times G_2$.

Solution:

(a) Since G_i is the Galois group of $L : K_i$, it operates trivially on K_i. Hence also $G_1 \cap G_2$ operates trivially on both K_1 and K_2, so $G_1 \cap G_2$ operates trivially on K_1K_2. Hence $K_1K_2 \subset L^{G_1 \cap G_2}$.

On the other hand, Since $\mathrm{Gal}(L : K_1K_2)$ is a subgroup of G_i, for both $i = 1, 2$, we have that $\mathrm{Gal}(L : K_1K_2) < G_1 \cap G_2$. By the Fundamental theorem of Galois theory $L^{G_1 \cap G_2} \subset K_1K_2$, and we obtain part (a).

(b) The group G_i operates trivially on K_i, for $i = 1, 2$. Then G_i operates trivially on $K_1 \cap K_2$ as well. Hence $\langle G_1 \cap G_2 \rangle$ operates trivially on $K_1 \cap K_2$, so that $K_1 \cap K_2 \subset L^{\langle G_1, G_2 \rangle}$.

Since G_i is a subgroup of $\langle G_1, G_2 \rangle$, we have $L^{\langle G_1, G_2 \rangle} \subset L^{G_i} = K_i$. Thus $L^{\langle G_1, G_2 \rangle} \subset K_1 \cap K_2$.

(c) Since $K_i : K$ is Galois, by the Fundamental theorem of Galois theory we obtain $G_i \triangleleft G$, which implies $\langle G_1, G_2 \rangle = G_1 G_2$. By part (b), we obtain $K = K_1 \cap K_2 = L^{\langle G_1, G_2 \rangle} = L^{G_1 G_2}$, so

$$G_1 G_2 = \mathrm{Gal}(L : K) = G \tag{1}$$

By part (a), we have $L = K_1 K_2 = L^{G_1 \cap G_2}$, so that

$$G_1 \cap G_2 = 1 \tag{2}$$

By equations (1) and (2), and the hint we have that $G \cong G_1 \times G_2$.

As for the hint, note that from Algebra I using (1) and (2) we know that $G = G_1 G_2$ is isomorphic to the internal semidirect product of G_1 and G_2:

$$G \cong G_1 \rtimes G_2.$$

But since both subgroups are normal, if $(n, h), (n', h') \in G_1 \rtimes G_2$ then in fact $n'h = hn'$. Indeed we have $n'hn'^{-1}h^{-1} = (n'hn'^{-1})h^{-1} \in (n'G_2 n'^{-1})G_2 = G_2$, and similarly $n'(hn'^{-1}h^{-1}) \in G_1 h G_1 h^{-1} = G_1$. Then $n'hn'^{-1}h^{-1} \in G_1 \cap G_2 = 1$, so $n'hn'^{-1}h^{-1} = 1$.

Hence

$$(n, h) * (n', h') = (n \cdot (hn'h^{-1}), hh') = (nn', hh'),$$

so the semidirect product above is actually a direct product: $G \cong G_1 \times G_2$.