D-MATH Algebra II FS 2024
Prof. Dr. Özlem Imamoglu

Solutions Exercise sheet 10

1. 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 $H_x \leqslant G := \mathrm{Gal}(L : K)$ 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 $K(x) = L$.

2. For p an odd prime number, let $\zeta := e^{2\pi i/p}$. Denote by C_i a cyclic group of order i.

(a) Show: $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. (*Hint:* Use Eisenstein criterion.)

(b) Show: $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) \cong C_{p-1}$.

Solution: (a) We have $\zeta^p = 1$, so ζ is a zero of the polynomial $X^p - 1$. From the decomposition

$$X^p - 1 = (X - 1)\left(X^{p-1} + X^{p-2} + \ldots + X + 1\right)$$

it follows that ζ is a zero of the polynomial $\varPhi_p := X^{p-1} + \ldots + X + 1 \in \mathbb{Z}[X]$.

We now want to show that $\varPhi_p$ is irreducible. From this it will follow that $\varPhi_p$ is the minimal polynomial of ζ over $\mathbb{Q}$, and thus that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \varPhi_p = p - 1$.

Next we will prove the irreducibility of $\varPhi_p$. With the substitution $X \leftrightarrow Y + 1$,

$$\varPhi_p(X) = \frac{X^p - 1}{X - 1} = \frac{(Y + 1)^p - 1}{Y} = \sum_{k=1}^{p} \binom{p}{k} Y^{k-1}.$$

So $\varPhi_p(Y)$ is a normalized polynomial of degree $p - 1$, and the k-th coefficient is $\binom{p}{k+1}$. Thus $\varPhi_p(Y)$ fulfills the requirements of the Eisenstein criterion for the prime number p, namely:

- The highest coefficient is 1, i.e. not divisible by p,

- for $0 \leqslant k \leqslant p - 2$, $\binom{p}{k+1}$ is divisible by p, so all lower coefficients are divisible by p,

- the constant term is $\binom{p}{1} = p$, i.e. not divisible by p^2.

(b) The p-th roots of unity form a group that is isomorphic to C_p. The restriction

$$\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) \to \mathrm{Aut}(\langle\zeta\rangle),\ \sigma \mapsto \sigma|_{\langle\zeta\rangle}$$

is well-defined, since all primitive roots of unity according to (a) have the same minimal polynomial. It is further injective, since an element of the Galois group is uniquely determined by the image of ζ. Furthermore, we know from Algebra I that $\mathrm{Aut}\,(C_p) \cong C_{p-1}$. Thus, $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ and $\mathrm{Aut}(\langle\zeta\rangle)$ have the same cardinality and the restriction is therefore also surjective, i.e. a group isomorphism.

3. Let L_f be the splitting field of $f = X^5 - 1$ over $\mathbb{Q}$.

(a) Determine $\mathrm{Gal}\,(L_f : \mathbb{Q})$.

(b) Determine all intermediate fields M with $\mathbb{Q} \subsetneq M \subsetneq L_f$.

(c) Let $\zeta := e^{\frac{2\pi i}{5}}$. Determine the minimum polynomial of $\zeta + \zeta^4$ over $\mathbb{Q}$.

Solution: (a) Because $f = (X-1)\,(1 + X + X^2 + X^3 + X^4)$ and because $(X-1) \in \mathbb{Q}[X]$ and $(1 + X + X^2 + X^3 + X^4)$ are irreducible, $|\mathrm{Gal}\,(L_f : \mathbb{Q})| = 4$. Let $\zeta := e^{\frac{2\pi i}{5}}$. For $1 \leqslant i \leqslant 4$, let $\alpha_i : L_f \to L_f$ with $\alpha_i : \zeta \mapsto \zeta^i$ be four different automorphisms. Because $\mathrm{ord}\,(\alpha_2) = 4$, we have $\mathrm{Gal}\,(L_f : \mathbb{Q}) = \langle \alpha_2 \rangle$, i.e. $\mathrm{Gal}\,(L_f : \mathbb{Q}) \cong C_4$.

(b) Note that the group C_4 has only one non-trivial subgroup, so the only non-trivial subgroup of $\mathrm{Gal}\,(L_f : \mathbb{Q})$ is $\langle \alpha_2^2 \rangle = \langle \alpha_4 \rangle$. Thus $M_0 := L_f^{\langle \alpha_4 \rangle}$ is the only non-trivial intermediate field, and because $\alpha_4 : \zeta \leftrightarrow \zeta^4$ and $\alpha_4 : \zeta^2 \leftrightarrow \zeta^3$ (i.e. the elements are being swapped), $M_0 = \mathbb{Q}\,(\zeta + \zeta^4) = \mathbb{Q}\,(\zeta^2 + \zeta^3)$. Note that $\zeta^5 = 1$, and that $(\zeta + \zeta^4)^2 = \zeta^2 + 2 + \zeta^3$ and $(\zeta^2 + \zeta^3)^2 = \zeta^4 + 2 + \zeta$.

(c) Since $\mathbb{Q}\,(\zeta + \zeta^4) = \mathbb{Q}\,(\zeta^2 + \zeta^3)$ and $[\mathbb{Q}\,(\zeta + \zeta^4) : \mathbb{Q}] = 2$, the minimum polynomial of $\zeta + \zeta^4$ over $\mathbb{Q}$ has, in addition to the zero $\zeta + \zeta^4$, also the zero $\zeta^2 + \zeta^3$, and thus

$$\big(X - (\zeta + \zeta^4)\big)\,\big(X - (\zeta 2 + \zeta^3)\big) = \\ X^2 - X(\underbrace{\zeta + \zeta^2 + \zeta^3 + \zeta^4}_{=-1}) + (\underbrace{\zeta + \zeta^2 + \zeta^3 + \zeta^4}_{=-1}) = -1 + X + X^2$$

is the minimum polynomial of $\zeta + \zeta^4$ (and also that of $\zeta^2 + \zeta^3$) over $\mathbb{Q}$.

4. For $n \geqslant 3$ let $\zeta \in \mathbb{C}$ be the primitive n-th root of unity. Prove:

$$\mathbb{Q}(\zeta) \cap \mathbb{R} = \mathbb{Q}(\zeta + \zeta^{-1})$$

and determine the degree $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})]$.

Solution: Let $K := \mathbb{Q}(\zeta) \cap \mathbb{R}$. Since ζ^{-1} and ζ are complex conjugates of each other, we have $\zeta + \zeta^{-1} \in \mathbb{R}$, so $\mathbb{Q}(\zeta + \zeta^{-1}) \subset K$. Since $\zeta \notin \mathbb{R}$ we have $K \subsetneq \mathbb{Q}(\zeta)$ and thus $[\mathbb{Q}(\zeta) : K] \geqslant 2$. On the other hand is ζ a zero of the quadratic polynomial $X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[X]$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$ and hence $\mathbb{Q}(\zeta + \zeta^{-1}) = K$.

5. Let K be a field, where the characteristic of K is not 2 and let $f(x) \in K[x]$, such that the zeros of f in a splitting field are $\alpha_1, \dots, \alpha_n$. Let

$$\delta = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j).$$

The *discriminant* $\varDelta(f)$ of f is defined as

$$\varDelta(f) = \delta^2.$$

Prove:

(a) $\Delta(f) \in K$.

(b) $\Delta(f) = 0$ if and only if it has a multiple zero.

(c) If $\Delta(f) \neq 0$, then $\Delta(f)$ is a perfect square in K if and only if the Galois group of f, interpreted as a group of permutations of the zeros of f, is contained in the alternating group A_n.

Solution:

(a) Let $\sigma \in S_n$ be a permutation acting by permutations on the zeros α_j of f. We can write σ as a product of permutations of order two. Note that a cycle of order two, say $(i'\ j')$ for $i' < j' \leqslant n$, sends δ to

$$\begin{aligned}(i'\ j')(\delta) &= \prod_{1\leqslant i<j\leqslant n} (\alpha_{(i'\ j')i} - \alpha_{(i'\ j')j}) \\ &= (\alpha_{j'} - \alpha_{i'}) \cdot \prod_{\substack{1\leqslant i<j\leqslant n \\ (i,j)\neq(i',j')}} (\alpha_i - \alpha_j) \\ &= - \prod_{1\leqslant i<j\leqslant n} (\alpha_i - \alpha_j),\end{aligned}$$

so if σ is applied to δ it sends δ to $\pm\delta$; the sign being $+$ if σ is an even permutation and $-$ if σ is odd. Therefore $\Delta(f) = \delta^2$ remains unchanged by any permutation in S_n, so it lies in K.

(b) This follows from the definition; if there were a multiple zero, one of the terms in the product of δ would be zero.

(c) Let G be the Galois group of f, considered as a subgroup of S_n for some integer n. If $\Delta(f)$ is a perfect square in K, then $\delta \in K$, so δ is fixed by G. We have seen in part (a) that odd permutations change the sign of δ to $-\delta$, and since $\mathrm{char}(K) \neq 2$, we have $\delta \neq -\delta$. Hence all permutations in G are even, so $G \leqslant A_n$.

On the other hand, if $G \leqslant A_n$ then for all $\sigma \in G$, $\sigma(\delta) = \delta$, so $\delta \in K$, and thus $\Delta(f)$ is a perfect square in K.