Algebra V - Galois Theory

Mock Exam

Fall 2024

Problem 1. *Indicate whether the statements that follow are true or false. You must justify your answers by providing a short explanation and/or a counterexample.*

(i) *If $\alpha \in \mathbb{R}$ is a root of some irreducible polynomial of degree four (over $\mathbb{Q}$), then α is constructible.*

This is false. If L denotes the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$ and α is constructible, then the order of $Gal(L/\mathbb{Q})$ must be a power of two. But we can certainly have $Gal(L/\mathbb{Q}) \simeq A_4$ or S_4, for example. Can you give a concrete example?

(ii) *If $K \subset F \subset L$ are fields such that L/F and F/K are algebraic, then L/K is algebraic.*

This is true. Pick $\alpha \in L$. Since α is algebraic over F we can consider $f(x) = \min(\alpha, F) = a_n x^n + \ldots + a_1 x + a_0$. Now, since the coefficients $a_i \in F$ are algebraic over K, considering $f_i(x) = \min(a_i, K)$, we have that

$$[K(\alpha) : K] \leq [K(\alpha, a_0, \ldots, a_n) : K] \leq deg f \cdot deg(f_n) \cdot \ldots \cdot deg(f_0).$$

(iii) *If $K(\alpha)/K$ is a finite field extension of odd degree, then $K(\alpha) = K(\alpha^2)$.*

This is true. First, note that $K \subset K(\alpha^2) \subset K(\alpha)$ and that α is root of $x^2 - \alpha^2 \in K(\alpha^2)[x]$. Thus, $[K(\alpha) : K(\alpha^2)] \leq 2$ and since $[K(\alpha) : K(\alpha^2)]$ must divide $[K(\alpha) : K]$ and the latter is an odd number, the equality follows.

(iv) *If L/K is a finite field extension such that $char(K)$ does not divide $[L : K]$, then every element of L is separable over K.*

This is true. We can show that a nonzero polynomial in $K[X]$ is separable if and only if it is relatively prime to its derivative in $K[X]$. In particular, for every field K, an irreducible polynomial in $K[X]$ is separable if and only if its derivative is not 0 in $K[X]$. This means that when K has characteristic 0, every irreducible in $K[X]$ is separable and when K has characteristic $p > 0$, an irreducible in $K[X]$ is separable if and only if it is not a polynomial in x^p.

Now, in our situation, we apply this to the minimal polynomial over K of an element $\alpha \in L$. Suppose that there exists some α with a minimal polynomial that is not separable. In that case, we can only be in characteristic p, and such polynomial must have a degree divisible by p, which divides $[L : K]$, contradicting our assumption.

(v) *There exist degree-two field extensions that are not normal.*

This is false. Every degree-two extension is normal. Let L/K be a degree-two extension. Pick $\alpha \in L$. Since α is algebraic, we can consider $\min(\alpha, K)$ which has degree $d \leq 2$. If $d = 1$, then this polynomial trivially splits (in $K[x] \subset L[x]$). If $d = 2$, then let $\beta \in \bar{K}$ be the second root and write $\min(\alpha, K) = x^2 + ax + b = (x - \alpha)(x - \beta)$. Then $\beta = -a - \alpha \in L$, and $\min(\alpha, K)$ splits in $L[x]$.

Problem 2. *Give an example of each of the following.*

(i) *A field extension L/K that is not solvable.*

It suffices to consider $K = \mathbb{Q}$ and $L = SF_{\mathbb{Q}}(f)$, where f is the polynomial $x^n - x + 1$, with $n \geq 5$. We have that $Gal(L/K) = S_n$, which is not solvable. Hence, the extension is not solvable (by the Abel criterion).

(ii) *Fields $K \subset F \subset L$ such that the extensions L/F and F/K are normal and L/K is not.*

One can take $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

(iii) *An irreducible polynomial $f \in \mathbb{Q}[x]$ such that $Gal(SF_{\mathbb{Q}}(f)/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$.*

It suffices to take $\alpha, \beta \in \mathbb{Q}$ such that α, β and $\alpha\beta$ are not squares in $\mathbb{Q}$. Then, cf. problem 6, the splitting field of $x^4 - 2(\alpha + \beta)x^2 + (\alpha - \beta)^2$ is $\mathbb{Q}(\sqrt{\alpha}, \sqrt{\beta}) = \mathbb{Q}(\sqrt{\alpha} + \sqrt{\beta})$. The automorphisms are determined by $\sqrt{\alpha} \to \pm\sqrt{\alpha}$ and $\sqrt{\beta} \to \pm\sqrt{\beta}$.

**In the actual exam, you must justify your answers.*

Problem 3.

(i) *Describe the splitting field $SF_{\mathbb{Q}}(f)$ of the polynomial $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ and compute the corresponding Galois group $Gal(SF_{\mathbb{Q}}(f)/\mathbb{Q})$.*

You should argue that $SF_{\mathbb{Q}}(f) = \mathbb{Q}(\sqrt[4]{2}, i)$ and $Gal(SF_{\mathbb{Q}}(f)/\mathbb{Q}) \simeq D_4$ (dihedral group with 8 elements).

(ii) *Give an example of a cubic polynomial in $\mathbb{Q}[x]$ such that $Gal(SF_{\mathbb{Q}}(f)/\mathbb{Q}) \simeq A_3$.*

Any polynomial of the form $x^3 - \alpha x + \alpha$, where $\alpha = k^2 + k + 7$ for some $k \in \mathbb{Z}$ (Lecture 11).

(iii) *Determine the splitting field of the polynomial $x^4 + 1$ over $\mathbb{F}_3$.*

Over $\mathbb{F}_3$ we have that

$$x^4 + 1 = (x^2 + x + 2)(x^2 - x + 2).$$

Now, irreducible polynomials of the same degree have the same splitting field over finite fields. So, the above tells us that the splitting field of $x^4 + 1$ is isomorphic to the splitting field of $x^2 + x + 2$, which is $\simeq \mathbb{F}_{3^2}$.

**In the actual exam, you must justify your answers.*

Problem 4. *Let p be a prime number in $\mathbb{Z}$ and let $L = SF_{\mathbb{Q}}(f)$ be the splitting field over $\mathbb{Q}$ of the polynomial $f(X) = x^n - p \in \mathbb{Q}[x]$, where $n \geq 3$. Prove that the group $Gal(L/\mathbb{Q})$ is never abelian, independent of n.*

Note that $L = \mathbb{Q}(\sqrt[n]{p}, \zeta_n \sqrt[n]{p}, \ldots, \zeta_n^{n-1} \sqrt[n]{p})$, where ζ_n is a primitive nth root of unity. Moreover, because $n \geq 3$, we have that $\mathbb{Q}(\sqrt[n]{p}) \neq L$ and the extension $\mathbb{Q}(\sqrt[n]{p})/\mathbb{Q}$ is not normal. Thus, $\mathrm{Gal}(L/\mathbb{Q})$ cannot be Abelian. Otherwise, any subgroup would be normal; hence, any intermediate field would be normal (over $\mathbb{Q}$).

Problem 5. *Let $p \geq 3$ be a prime number, ζ_p a (primitive) pth root of unity, and $L = \mathbb{Q}(\zeta_p)$.*

(i) Prove that $L/\mathbb{Q}$ is Galois and determine the corresponding Galois group.

We have that $L = SF_{\mathbb{Q}}(x^p - 1)$, hence L is normal. The extension is separable since we are in characteristic zero. Now, $Gal(L/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^{\times}$. So, the extension is cyclic.

(ii) Prove that $N_{L/\mathbb{Q}}(\zeta_p) = 1$ and deduce that for each generator σ of $Gal(L/\mathbb{Q})$, there exists $a \in L$ such that $\zeta_p = \dfrac{a}{\sigma(a)}$.

The set $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$ gives a basis for L. Multiplication by ζ_p defines a linear map $L \to L$ whose matrix representation in this basis is

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -1 \\ 1 & 0 & 0 & \cdots & 0 & -1 \\ 0 & 1 & 0 & \cdots & 0 & -1 \\ 0 & 0 & 1 & \cdots & 0 & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{pmatrix}$$

We have seen (Worksheet 3) that $N_{L/\mathbb{Q}}(\zeta_p)$ is simply the determinant of this linear map. We can simply use Laplace expansion along the first row to see that the determinant equals one ($= (-1)^{p-1}$). The conclusion then follows from Hilbert's 90.

Problem 6. *Let L/K be a field extension of degree four, and assume that $char(K) \neq 2$. Prove that L contains an intermediate subfield F with $[L : F] = 2$ if and only if $L = K(\gamma)$, where γ is a root of an irreducible polynomial of the form $x^4 + ax^2 + b \in K[x]$.*

$\Rightarrow$ If $\exists\ K \subset F \subset L$ such that $[L : F] = 2$, then we can find $\alpha \in K$ and $\beta \in F$ such that $L = F(\sqrt{\beta})$ and $F = K(\sqrt{\alpha})$. Thus, $L = K(\sqrt{\alpha}, \sqrt{\beta})$. Now, $[K(\sqrt{\beta}) : K] = 2$ or 4. In the first case, we may assume that $\beta \in K$ and then $L = K(\gamma)$ for $\gamma = \sqrt{\alpha} + \sqrt{\beta}$ a root of $x^4 - 2(\alpha + \beta)x^2 + (\alpha - \beta)^2$. In the second case, we must have that $\beta = c + d\sqrt{\alpha}$ and $L = K(\gamma)$ for $\gamma = \sqrt{\beta}$ a root of $x^4 - 2cx^2 + c^2 - d^2\alpha$.

$\Leftarrow$ Note that γ is of the form $\pm\sqrt{\dfrac{-a \pm \sqrt{a^2 - 4b}}{2}}$. Since L/K has degree four, the polynomial must be irreducible, and $a^2 - 4b$ cannot be a square in K. And since $\sqrt{a^2 - 4b} \in L$, we have that $F = K(\sqrt{a^2 - 4b})$ is an intermediate field with $[L : F] = 2$.