Homework #9. Algebra 2. Name: Gustavo Chaparro-Sumalave.

Prob 1. Let E/F be a finite field extension. Prove that every element of E is algebraic over F.

Solution: Let $\alpha \in E$. Let $n := \min\{m : \{1, \alpha, \dots, \alpha^m\}$ is linearly independent$/F\}$. Since E/F is a finite field extension, n is a well defined non-negative integer. Then $\{1, \alpha, \dots, \alpha^{n+1}\}$ is linearly dependent, so there are $a_i \in F$ such that $a_0 1 + a_1 \alpha + \cdots + a_{m+1}\alpha^{m+1} = 0$, not all of the a_i's being zero.

Hence $I_\alpha \neq (0)$ and α is algebraic.

Notation from Lecture notes.

Prob. 2. Let E/F be a field extension. Consider the set E^{alg} of all elements of E which are algebraic over F. Prove that E^{alg} is a field containing F.

Solution. Let $\alpha, \beta \in E^{alg}$. By Thm (?) (Page 6, Lect. 26), we have $(F(\alpha):F) < \infty$ and $(F(\beta):F) < \infty$. Since $(F(\alpha,\beta):F) < \infty$ (because $(F(\alpha,\beta):F) \leq (F(\alpha):F)(F(\beta):F)$; if $\{\alpha_1, \dots, \alpha_m\}$ and $\{\beta_1, \dots, \beta_n\}$ are bases of $F(\alpha)$ and $F(\beta)$ as F-vector spaces, $\{\alpha_i \beta_j : i = 1, \dots, m; j = 1, \dots, n\}$ spans $F(\alpha, \beta)$ as F-vector space) and we have the towers of fields $F \subset F(\alpha+\beta) \subset F(\alpha,\beta)$ and $F \subset F(\alpha\beta) \subset F(\alpha,\beta)$, it follows that $\alpha+\beta$ and $\alpha\beta$ are algebraic. Hence E^{alg} is closed under addition and multiplication. The two operations inherit the field properties from E, so E^{alg} is a field.

Finally, for any $\alpha \in F$, $x - \alpha \in F[x]$ is its minimal polynomial, so $\alpha \in E^{alg}$ and $E^{alg} \supseteq F$.

Prob. 3 Let F be a field and $p(x) \in F[x]$. Let E be the splitting field of $p(x)$ over F. Prove that $(E:F)$ divides $n!$.

Solution: We apply induction on n. If $n=1$, $p(x) = ax+b$ for some $a,b \in F$. Hence $p(x) = a\left(x + \frac{b}{a}\right)$ over F and then $E = F$, so $(E:F) = 1 \mid 1!$.

Let $n \geq 2$. If $p(x)$ is irreducible over F and $E = F(\alpha_1, \ldots, \alpha_n)$ so that $p(x) = \underbrace{a}_{\in F}(x-\alpha_1)\cdots(x-\alpha_n)$ in $E[x]$, let us write $p(x)$ as $g(x)(x-\alpha_1)$ in $F(\alpha_1)[x]$ $\left(g(x) \in F(\alpha_1)[x] \right)$.

Then
$$(E:F) = \underbrace{(E:F(\alpha_1))}_{\text{divides } (n-1)!\text{, by induction applied to } g(x)} (F(\alpha_1):F) = (E:F(\alpha_1))\underbrace{n}_{p(x) \text{ is irreducible over } F} \mid n!.$$

If $p(x)$ is not irreducible over F, let $p(x) \underset{\text{in } F[x]}{=} \tilde{p}(x)\, p_1(x)$ with $\tilde{p}(x)$ irreducible over F. Let $\tilde{E}$ be the splitting field of $\tilde{p}(x)$ over F $(\tilde{E} \subset E)$. Then, if $\deg(\tilde{p}(x)) = m$, we have

$$(E:F) = \underbrace{(E:\tilde{E})}_{\text{divides } (n-m)!} \underbrace{(\tilde{E}:F)}_{\text{divides } m!} \mid n! \quad \text{as } \binom{n}{m} \in \mathbb{Z}.$$

induction $\Rightarrow$

In any case, $(E:F)$ divides $n!$ as we wanted.

2

Prob. 8 Let $f(x) = x^6 + x^3 + 1 \in \mathbb{Q}[x]$. Prove that $f(x)$ is irreducible. How many morphisms of fields are there from $\mathbb{Q}[x]/(f(x))$ to $\mathbb{C}$?

Solution: If $f(x)$ were reducible over $\mathbb{Q}[x]$ and $f(x) = h(x)g(x)$ with $\deg(g(x)), \deg(h(x)) < \deg(f(x))$, then $f(x+1) = h(x+1)g(x+1)$ would imply that $f(x+1)$ is not irreducible. However,

$$f(x+1) = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3,$$ and applying Eisenstein's criterion with $p=3$, we find that $f(x+1)$ is irreducible.

There are six morphisms of fields from $\mathbb{Q}[x]/(f(x))$ to $\mathbb{C}$:

Let E be the splitting field of $f(x)$ and let $\alpha \in E$ be one root of $f(x)$. We know $\mathbb{Q}[x]/(f(x)) \cong \mathbb{Q}(\alpha)$ and any field homomorphism $\mathbb{Q}(\alpha) \xrightarrow{\varphi} \mathbb{C}$ fixes $\mathbb{Q}$ (as $1 \mapsto 1$) and it is determined by the image of α. But $\alpha^6 + \alpha^3 + 1 = 0$ implies $\varphi(\alpha)^6 + \varphi(\alpha)^3 + 1 = 0$, so $\varphi(\alpha)$ is root of $x^6 + x^3 + 1 \in \mathbb{C}[x]$.

Let $t := x^3$, so $0 = x^6 + x^3 + 1 = t^2 + t + 1$ implies $t = e^{\frac{2\pi i}{3}}$ or $e^{\frac{4\pi i}{3}}$.

Then $x = e^{\frac{2\pi i}{9}}, -e^{\frac{5\pi i}{9}}, e^{\frac{8\pi i}{9}}, -e^{\frac{\pi i}{9}}, e^{\frac{4\pi i}{9}}, -e^{\frac{7\pi i}{9}}$. There are six different roots of $x^6 + x^3 + 1$ in $\mathbb{C}$. Let β be one of them.

If $\varphi(\alpha) = \beta$, we can consider φ as a field homomorphism $\mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\beta)$ (unique field isomorphism, Thm. 26.7).

Letting β vary we get the six morphisms

$$\mathbb{Q}[x]/(f(x)) \longrightarrow \mathbb{Q}(\beta) \subset \mathbb{C}.$$

Prob 9. Let E be the splitting extension of $p(x) = x^5 - 7$ over $\mathbb{Q}$. Compute $(E:\mathbb{Q})$.

Solution: Let $7^{\frac{1}{5}}$ be the real solution of $x^5 - 7 = 0$. Let $w = e^{\frac{2\pi i}{5}}$, a primitive 5^{th} root of unity. Then $7^{\frac{1}{5}}, 7^{\frac{1}{5}}w, 7^{\frac{1}{5}}w^2, 7^{\frac{1}{5}}w^3, 7^{\frac{1}{5}}w^4$ are all the roots of $p(x)$ in $\mathbb{Q}(7^{\frac{1}{5}}, w) (= E)$.

We know $w^5 - 1 = 0$ and that $x^5 - 1 = (x-1)\underbrace{(x^4+x^3+x^2+x+1)}_{=:g(x)}$.

The polynomial $g(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion applied to $g(x+1) = x^4 + 5x^3 + 10x^2 + 10x + 5$ with $p=5$, so $(\mathbb{Q}(w):\mathbb{Q}) = 4$.

The polynomial $p(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion applied with $p=7$, so $(\mathbb{Q}(7^{\frac{1}{5}}):\mathbb{Q}) = 5$.

By problem 4, since $\gcd(4,5) = 1$, $(E:\mathbb{Q}) = 20$.

The first part of problem 4 follows by what it is mentioned in the solution to problem 2, so we have $(\mathbb{Q}(7^{\frac{1}{5}}, w):\mathbb{Q}) \leq (\mathbb{Q}(7^{\frac{1}{5}}):\mathbb{Q})(\mathbb{Q}(w):\mathbb{Q}) = 20$. On the other hand, both 4 and 5 divide $(E:\mathbb{Q})$ by Thm 26.2, so $(E:\mathbb{Q})$ is divisible by 20. Hence $(E:\mathbb{Q}) = 20$.

very nice!

$\frac{50}{50}$ Génial!