Fields & Galois Theory - Midterm exam - 02/11/15.

Problem 1 See coursenotes.

Problem 2 $P \in k[X]$ $\deg P = n \geq 1$.

(1) P irreducible.

(a) Stem field of P: $k[X]/(P)$

(b) K/k extension.

If k contains a root α for P, define

$$\varphi : k[X] \longrightarrow K$$
$$Q(X) \longmapsto Q(\alpha)$$

Its kernel is $\ker\varphi = \{Q \in k[X] \ Q(\alpha) = 0\}$ but P being irreducible, it is the minimal polynomial of α and therefore $\ker\varphi = (P)$.

This implies that φ factors through an injective morphism

$$k[X]/(P) \hookrightarrow K.$$

(2) Suppose P is reducible. Then it decomposes $P = QR$ with $\deg Q, \deg R > 0$ and $\deg Q + \deg R = n$.

We may assume that $\deg Q \leq n/2$ (WLOG)

Let A be an irreducible factor of Q.

Then $E := k[X]/A$ is a field with degree $\leq n/2$

The image $\bar{X}$ of X in E satisfies $P(\bar{X}) = 0$.

(3) $k = \mathbb{F}_p$.

(a) $\Leftarrow$ If P reducible it has a root in some extension of degree $\leq n/2$ by (2)

But all extensions of $\mathbb{F}_p$ are of the form

$\mathbb{F}_p^d$ for $d \geq 1$. Therefore P has a root in $\mathbb{F}_p^d$ for some $d \leq n/2$.

$\Rightarrow$ Suppose P is irreducible. If P has a root in $\mathbb{F}_p^d$ for some $d \leq n/2$ then $\mathbb{F}_p[X]/(P) \hookrightarrow \mathbb{F}_p^d$ by (1)(b)

$= \mathbb{F}_p^n$

Contradiction since $n > d$.

(b) The GCD of P and $X^{p^d} - X$ can be computed in any extension of $\mathbb{F}_p$ (it will be the same result).

In $\mathbb{F}_p^d$, $X^{p^d} - X = \prod_{\alpha \in \mathbb{F}_p^d} (X - \alpha)$

Therefore, for $1 \leq d \leq n/2$,

$GCD(P, X^{p^d} - X) = 1 \iff \forall \alpha \in \mathbb{F}_p^d$, $X - \alpha$ does not divide P

$\iff$ P has no root in $\mathbb{F}_p^d$.

Conclude using (a).

Problem 3:

(1) Define $\sigma_n \longrightarrow Aut(\mathbb{Q}(X_1, \dots, X_n))$

$\sigma \longmapsto \varphi_\sigma$

where $\varphi_\sigma : \mathbb{Q}(X_1, \dots, X_n) \longrightarrow \mathbb{Q}(X_1, \dots X_n)$

$f \longmapsto f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$

It is well defined (φ_σ is an automorphism)

It is a morphism of groups. ($\varphi_{\sigma \circ \sigma'} = \varphi_\sigma \circ \varphi_{\sigma'}$)

It is injective. $\varphi_\sigma = id \Rightarrow \varphi_\sigma(X_i) = X_i \ \forall i$

$\Rightarrow \sigma(i) = i \ \forall i$

$\Rightarrow \sigma = id$.

So $\mathfrak{S}_n \simeq \operatorname{Im}\varphi$ which is a subgroup of $\operatorname{Aut}(\mathbb{Q}(X_1, \dots, X_n))$.

(2) G a group $|G| = n$.

(a) Let $F : G \longrightarrow \operatorname{Bij}(G)$

$$g \longmapsto F_g := \left[\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gx \end{array}\right]$$

where $\operatorname{Bij}(G)$ is the set of bijections $G \to G$.
Since $|G| = n$, we have $\operatorname{Bij}(G) \simeq \mathfrak{S}_n$ as a group.

- F is a morphism of groups.
- $\operatorname{Ker} F = \{ g \in G \mid F_g = id_G \}$

$= \{ g \in G \mid gx = x \ \forall x \in G \}$

$= \{ 1_G \}$ so F is injective.

(b) G can be identified with a subgroup of $\mathfrak{S}_n$ which can be identified with a subgroup of $\operatorname{Aut}(\mathbb{Q}(X_1, \dots, X_n))$. So G can be seen as a subgroup of $\operatorname{Aut}(\mathbb{Q}(X_1, \dots, X_n))$.

$E := \mathbb{Q}(X_1, \dots, X_n)$ is perfect since it has characteristic zero.

E / E^G is Galois with Galois group G.