PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 8 (Mar 14 – Apr 4)

1 (5+5+5) Let $K \subseteq L$ be a splitting field extension for some $f \in K[t] \setminus K$. Then the following are equivalent:
(i) f has a repeated root over L;
(ii) $\exists \alpha \in L$ s.t. $0 = f(\alpha) = (\mathcal{D}f)(\alpha)$;
(iii) $\exists g \in K[t]$, $\deg g \geq 1$ s.t. g divides both f and $\mathcal{D}f$.

2 (5) Let K be a field, $\mathrm{char}(K) = p > 0$ and $f \in K[t^p]$ is an irreducible polynomial over K. Prove that f is inseparable.

3 (10) Let K be a field, $\mathrm{char}(K) = p > 0$ and $f \in K[t^p]$ is an irreducible polynomial over K. Prove that there is $g \in K[t]$ and a non-negative n such that $f(t) = g(t^{p^n})$ and g is an irreducible and separable polynomial.

4 (10) Prove that $\prod_{\alpha \in \mathbb{F}_q^*} \alpha = -1$.

5 (5+5+5+5) a) Let $\alpha \in \mathbb{F}_q$ and $\alpha = \beta - \beta^p$ for some $\beta \in \mathbb{F}_q$. Prove that $\mathrm{Tr}(\alpha) = 0$.

b) Let $\alpha \in \mathbb{F}_q$ and $\alpha = \gamma^{1-p}$ for some nonzero $\gamma \in \mathbb{F}_q$. Prove that $\mathrm{Norm}(\alpha) = 1$.

c) Let $\alpha \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. Prove that $\mathrm{Tr}(\alpha) = n\alpha$.

d) Let $\alpha \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. Prove that $\mathrm{Norm}(\alpha) = \alpha^n$.

6 The midterm exam will be on Thursday the 27th!

Solutions

General remark. If there is a typo in any task, then the maximum score will be awarded for that task.

1 (5+5+5) Let $K \subseteq L$ be a splitting field extension for some $f \in K[t] \setminus K$. Then the following are equivalent:
(i) f has a repeated root over L;
(ii) $\exists \alpha \in L$ s.t. $0 = f(\alpha) = (\mathcal{D}f)(\alpha)$;
(iii) $\exists g \in K[t]$, $\deg g \geq 1$ s.t. g divides both f and $\mathcal{D}f$.

Solution. $(i) \implies (ii)$ If f has a repeated root α, then $f(x) = (x-\alpha)^s g(x)$, where $s > 1$ and thus $\mathcal{D}f = (x-\alpha)^{s-1}(sg(x) + (x-\alpha)\mathcal{D}g)$ thanks to the Leibnitz rule. Thus $(\mathcal{D}f)(\alpha) = 0$.

$(ii) \implies (iii)$ If $0 = f(\alpha) = (\mathcal{D}f)(\alpha)$, then μ_α^K, $\deg(\mu_\alpha^K) \geq 1$ divides both f and $\mathcal{D}f$.

$(iii) \implies (i)$ Suppose that $\exists g \in K[t]$, $\deg g \geq 1$ s.t. g divides both f and $\mathcal{D}f$. Let α be a root of g. Then $f(t) = (t-\alpha)g_*(t)$, $g_* \in L[t]$ and $\mathcal{D}f = g_*(t) + (t-\alpha)\mathcal{D}g_*(t)$. We know that $g|\mathcal{D}f$ and hence $(t-\alpha)$ divides g_*. It follows that $(t-\alpha)^2$ divides $f(t)$ as required.

2 (5) Let K be a field, $\mathrm{char}(K) = p > 0$ and $f \in K[t^p]$ is an irreducible polynomial over K. Prove that f is inseparable.

Solution. We have $\mathcal{D}f = 0$ thus by the previous question f has multiple roots and therefore f is inseparable over K.

3 (10) Let K be a field, $\mathrm{char}(K) = p > 0$ and $f \in K[t^p]$ is an irreducible polynomial over K. Prove that there is $g \in K[t]$ and a non-negative n such that $f(t) = g(t^{p^n})$ and g is an irreducible and separable polynomial.

Solution. Let n be the largest non-negative integer having the property that $f(t) = g(t^{p^n})$, i.e. $f \in K[t^{p^n}]$. By our criterion of inseparability (Theorem 1 of Lecture 16) we see that if g is inseparable, then $g = h(t^p)$ and hence $f \in K[t^{p^{n+1}}]$, contradicting our choice of n. Thus g is separable. Finally, if g is reducible, then f is reducible and this is a contradiction.

4 (10) Prove that $\prod_{\alpha \in \mathbb{F}_q^*} \alpha = -1$.

Solution. Any nonzero $\alpha \in \mathbb{F}_q^*$ has the inverse element $\beta = \alpha^{-1}$ that is $\alpha\beta = 1$. We have $\beta = \alpha$ iff $\alpha^2 = 1$ and therefore $\alpha = \pm 1$. Splitting all elements $\alpha \in \mathbb{F}_q^*$ into pairs (α, β), we obtain

$$\prod_{\alpha \in \mathbb{F}_q^*} \alpha = \prod_{\alpha \in \mathbb{F}_q^*,\, \alpha \neq \pm 1} \alpha \cdot 1 \cdot (-1) = 1 \cdot 1 \cdot (-1) = -1$$

as required.

5 (5+5+5+5) a) Let $\alpha \in \mathbb{F}_q$ and $\alpha = \beta - \beta^p$ for some $\beta \in \mathbb{F}_q$. Prove that $\mathrm{Tr}(\alpha) = 0$.

b) Let $\alpha \in \mathbb{F}_q$ and $\alpha = \gamma^{1-p}$ for some nonzero $\gamma \in \mathbb{F}_q$. Prove that $\mathrm{Norm}(\alpha) = 1$.

c) Let $\alpha \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. Prove that $\mathrm{Tr}(\alpha) = n\alpha$.

d) Let $\alpha \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. Prove that $\mathrm{Norm}(\alpha) = \alpha^n$.

Solution. a)–b) This is a direct calculation. c)–d) Use the property of the Frobenius automorphism φ, namely, $\varphi(\alpha) = \alpha$ iff $\alpha \in \mathbb{F}_p$.

6 The midterm exam will be on Thursday the 27th!