HW4

Solutions

HW4

(1) Suppose g is a monic irreducible factor of $x^{p^p}-x$ in $\mathbb{Z}_p[x]$. Let L be a field extension with $[L:\mathbb{Z}_p]=p$. We know that L/K is SFE of $x^{p^p}-x$, which means L contains a root of g namely α. Since g monic, irreducible, $g=m_\alpha \in \mathbb{Z}_p[x]$. $[k(\alpha):k]=\deg g \mid p$. so $\deg g=1$ or p. OTOH, $\forall \alpha \in \mathbb{Z}_p$, $\alpha^p=\alpha$, then $\alpha^{p^p}=\alpha \Rightarrow x-\alpha \mid x^{p^p}-x$. $\forall g$ monic, irreducible, $\deg g=p$, $\exists!$ field of order p^p. $\mathbb{Z}_p[x]/(g) \cong L$, then $\beta^{p^p}-\beta=0$, $g=m_\beta \mid x^{p^p}-x$. Therefore, $x^{p^p}-x=\prod_{\alpha \in \mathbb{Z}_p}(x-\alpha)\, g_{\substack{\text{monic}\\ \text{irred}\\ \deg g=p}} g(x)$.

(2) $p \nmid q-1$, $\exists m,n \in \mathbb{Z}$ s.t. $mp+n(q-1)=1$. Let L be the SFE of x^p-1 and one of its roots in $L \setminus \mathbb{Z}_p$ is r, so $r^p=1$, $r \neq 1$. Notice that $(r^k)^p=1$. $(1 \le k \le p-1)$ and $r^{k_1}=r^{k_2} \Leftrightarrow r^{k_1-k_2}=1 \Leftrightarrow p \mid k_1-k_2 \Leftrightarrow k_1=k_2$ for $1 \le k_1, k_2 \le p$, so $1, r, \cdots, r^{p-1}$ are p distinct roots of x^p-1. $x^p-1=(x-1)(x-r)\cdots(x-r^{p-1})$. $L=\mathbb{Z}_q(x)$. $\forall a \in \mathbb{Z}_q^*$, $(a_r)^{mp}$ $=a^{mp}r^{mp}=a^{-p}=a^{1-n(q-1)}=a$. $\{r^k(ar)^m\}_{k=0 \text{ to } p-1}$ are roots of x^p-a. x^p-a splits in L. OTOH, if x^p-a splits in $L' \subset L$, $[ar]^m \subset L'$, $r(ar)^m \subset L'$, thus $r \in L'$. $L=\mathbb{Z}_p(r) \subset L'$ $L'=L$. Thus L is a splitting field extension for each of the polynomial x^p-a.

(3) M/K is finite by the Tower Law. So if K is a finite field, so is M and M/K is simple for that it has finitely many intermediate field. Assume K is an infinite field and since L/K is finite and separable, it is also simple. i.e. $L=K(\alpha)$ for some $\alpha \in L$ and by defination $M=L(\beta)$ $=K(\alpha,\beta)$ for some $\beta \in M$.

Let N/K be a splitting field extension of $m_\alpha m_\beta$ over K.

$m_\alpha=\prod_{i=1}^{n}(x-\alpha_i)$ where $\alpha_1=\alpha$, $m_\beta=\prod_{i=1}^{m}(x-\beta_i)$, where $\beta_1=\beta$

Let $\lambda \in K \setminus \left\{ \frac{\beta-\beta_j}{\alpha-\alpha_i} \mid j=1,\cdots,m,\ i=2,\cdots,n \right\}$.

Note $\lambda \neq 0$ and the denominator does not vanish for the separability of α. Now let $L'=K(\beta+\lambda\alpha)$ and $h(x)=m_\beta(\beta-\lambda\alpha+\lambda x) \in L'[x]$.

The roots of $h(x)$ are α and $(\beta_i-\beta+\lambda\alpha)/\lambda$ for $i=2,\cdots,n$ so that h splits over N.
Claim: $\alpha\in L'$.
Since there is a unique monic highest common factor of m_α and h in $L'[x]$. It suffices to show such factor is $x-\alpha$.
Let d be the monic h.c.f. of m_α and h in $L[x]$ and d' be the monic h.c.f of m_α and h in $N[x]$. It follows that $d|d'$ in $N[x]$. However, there are $p,q\in L[x]$ such that $d=pm_\alpha+qh$ and $d'|m_\alpha, h$ in $N[x]$, so $d'|d$. Thus d and d' are associates in N and since they are both monic, $d=d'$. Next we want to show $d'=(x-\alpha)$. Note that $(x-\alpha)|d'$ since $h(\alpha)=m_\beta(\beta-\lambda\alpha+\lambda\alpha)=m_\beta(\beta)=0$. Suppose $d'\neq(x-\alpha)$, then we may have another monic irreducible divisor of d', say p. Since $d|m_\alpha$ and α is separable, $p\neq(x-\alpha)$.
Therefore, $p=x-\alpha_i=(x-(\beta_j-\beta+\lambda\alpha)/\lambda)$ for some $i,j\in\{2,\cdots,n\}$, or that $\alpha_i=(\beta_j-\beta+\lambda\alpha)/\lambda$. So $\alpha_i\lambda=\beta_j-\beta+\lambda\alpha$ or $(\alpha_i-\alpha)\lambda=\beta_j-\beta$ namely, $\lambda=\frac{\beta_j-\beta}{\alpha_i-\alpha}$ for some $2\le i,j\le n$. contradiction!

4. $\forall m,n\in\mathbb{N}$, $m\neq n$ (WLOG, let $m<n$) if $K(t^m)\cong K(t^n)$, then we have $t^n=\frac{f(t^m)}{g(t^m)}$. $t^m\cdot g(t^m)=f(t^m)$. Consider $F(x)=f(x^n)-x^m g(x^n)$. According to $m<n$, all the terms of $f(x^m)$ has degree $n-d_i$, all the terms of $x^m g(x^m)$ has degree $n-d_j+m$ and they cannot be cancelled out. Since $g(x)\neq 0$, we know that $F(x)\neq 0$. and t is a root of $F(x)$ in K. This is contradict to t is transcendental in K.
Thus $\{K(t^n)\}_{n\in\mathbb{N}}$ are distinct intermediate fields so there are infinitely many of them.

(5) Define G^i by $G^1 = G$, $G^i = (G^{i-1}, G)$. The sequence of normal subgroups $G^1 \supset G^2 \supset G^3 \supset \cdots$ is called the *lower central series* for G. G is called *nilpotent* if there exists an integer k such that $G^k = 1$. Show that if G is nilpotent, then it is solvable. Give an example to show that the converse does not hold.

Proof:

Suppose G is nilpotent and $G^{(1)} = (G, G) = G^1$ and let us suppose $G^{(i)} \subset G^i$, we have $G^{(i+1)} = (G^{(i)}, G^{(i)}) \subset (G^i, G) \subset G^{i+1}$. By induction, $G^{(i)} \subset G^i$ holds for all i and thus $G^{(k)} \subset G^k = 1$ for some k and G is solvable.

Take $G = \mathfrak{S}_3$ being solvable and since $(\mathfrak{A}_3, \mathfrak{S}_3) = \mathfrak{A}_3$, the lower central series does not go to 1 and $\mathfrak{S}_3$ is not nilpotent. □

(6) If G is a group define the *upper central series* $1 \subset C_1 \subset C_2 \subset \cdots$ by $C_1 = C(G)$, and C_i, the normal subgroup such that C_i/C_{i-1} is the center of G/C_{i-1}. Show that a finite group G is nilpotent iff the upper central series ends in a finite number of steps with G ($G = C_k$ for some k).

Proof:

($\Leftarrow$) Suppose the upper central series terminates after finite steps: $1 \subset C_1 \subset \cdots \subset C_k = G$. Let $G = G^0 \supset G^1 \supset \cdots$ be the lower central series. Suppose $C_i \supset G^{k-i}$ and then $(G, C_i) \supset (G, G^{k-i})$. Note C_i/C_{i-1} is the center of G/C_{i-1}, we have $C_{i-1} \supset (G, C_i) \supset (G, G^{k-i}) = G^{k-i+1}$. Hence by induction we have $C_i \supset G^{k-i}$ for all i, $G^k \subset C_0 = 1$ and G is therefore nilpotent.

($\Rightarrow$)

(7) Prove that if $\varphi(n)$ is the Euler φ-function then

$$\varphi(n) = \sum_{d|n} \mu(n/d)d.$$

Proof: From the Möbius inversion formula if $g(n) = \sum_{d|n} \varphi(d)$, then

$$\varphi(n) = \sum_{d|n} \mu(n/d)g(d).$$

Together with Euler's classical formula, $g(n) = n$; hence we conclude that $\varphi(n) = \sum_{d|n} \mu(n/d)d$. □

(8) Find a primitive element for splitting field over $\mathbb{Q}$ of $x^5 - 2$.

Answer:

Let ξ_5 be a primitive 5-th root of unity and the Galois group of $x^5 - 2$ over $\mathbb{Q}$ are permutations of roots. Note that every permutation σ is determined by $\sigma(\sqrt{2})$ and $\sigma(\xi_5)$. Put $\alpha = \sqrt{2} + \xi_5$ and the only σ fixes α is the identity. So $\mathbb{Q}(\alpha)$ is the splitting field of $x^5 - 2$ and α is a primitive element.