SOLUTION OF ALGEBRA-IV MID SEMESTRAL EXAM, 2011-12

Solution to problem 1

Let f be a field automorphism. First of all we prove that f restricted on $\mathbb{Q}$ is identity. For that observe that

$$f(n.\frac{1}{n}) = f(1) = 1$$

that implies that

$$nf(\frac{1}{n}) = 1$$

which gives

$$f(\frac{1}{n}) = \frac{1}{n} \; .$$

Therefore it follows that

$$f(\frac{m}{n}) = \frac{m}{n} \; .$$

Now we prove that if $x \geq 0$ then $f(x) \geq 0$. For that we write

$$x = (\sqrt{x})^2$$

so we get that

$$f(x) = f(\sqrt{x})^2 \geq 0 \; .$$

Now take a sequence x_n that converges to 0. Then we have to prove that $f(x_n)$ converges to 0. For that we observe that by the Archimedian property of the real line and the fact that the sequence x_n goes to 0, we always get a sequence of integers a_n such that

$$\frac{1}{a_{n+1}} < x_n < \frac{1}{a_n}$$

applying f we get that

$$\frac{1}{a_{n+1}} < f(x_n) < \frac{1}{a_n}$$

so $f(x_n)$ goes to zero. Now since $\mathbb{Q}$ is dense in $\mathbb{R}$. Given any $a \in \mathbb{R}$, we have a sequence of rational numbers x_n converging to a. Then we have by continuity of f that $f(x_n)$ tends to $f(a)$. But $f(x_n) = x_n$, so by the uniqueness of limit we have

$$f(a) = a \; .$$

Hence we are done.

Solution to problem 2

The isomorphism extension theorem states that any isomorphism $\phi : E \to F$ can be extended uniquely to an algebraic extension E' of E to an algebraic extension F' of F.

The splitting field of $x^3 - 5$ is the finite extension of $\mathbb{Q}$ generated by $\sqrt[3]{5}$ and ρ, where ρ is a primitive 3-rd root of unity. Since we can write this splitting field as $\mathbb{Q}(\sqrt[3]{5})(\sqrt[3]{5}\rho)$, which is a degree 6 extension of $\mathbb{Q}$. So there will be atmost 6 automorphism in 6, since the extension is Galois there will be exactly 6 automorphisms. Define

$$\sigma(\sqrt[3]{5}) = \rho\sqrt[3]{5}, \quad \sigma(\rho) = \rho$$

and

$$\tau(\sqrt[3]{5}) = \sqrt[3]{5}, \quad \tau(\rho) = \rho^2 \ .$$

We can check that

$$\sigma^3 = id, \quad \tau^2 = id$$

and

$$\sigma\tau = \tau\sigma^2 \ .$$

So the Galois group is S_3.

<u>Solution to problem 3</u>

a)Since K, L are finite Galois extensions of F. We can write $K = F(a_1, \cdots, a_n)$ and $L = F(b_1, \cdots, b_m)$. Then $KL = F(a_1, \cdots, a_n, b_1, \cdots, b_m)$ since a_i, b_j's are roots of a minimal separable polynomial m_{a_i}, m_{b_j}'s we get that any element α in KL is the root of a separable polynomial in $F[x]$. Since K is the splitting field of $m'_{a_i}s$ and L is the splitting field of $m'_{b_j}s$ we get that KL is the splitting field of m_{a_i}, m_{b_j}'s.

b)Define the group homomorphism from $Gal(KL/F)$ to $Gal(K/F) \times Gal(L/F)$ defined by

$$\sigma \mapsto (\sigma|_K, \sigma|_L) \ .$$

It can be checked that the above map is a homomorphism. Suppose that

$$\sigma|_K = id, \quad \sigma|_L = id \ .$$

Then $\sigma = id$, this is because we write any element in KL as

$$\prod_i a_i^{n_i} \prod_j b_j^{m_j}$$

and σ acts identically on each of these factors. So the homomorphism is injective.

c)The image lies in the subgroup H of $Gal(K|F) \times Gal(L|F)$ given by

$$\{(\sigma, \tau) | \sigma|_{K\cap L} = \tau|_{K\cap L}\} \ .$$

Since $(\sigma|_K)_{K\cap L} = \sigma|_{K\cap L} = (\sigma|_L)_{K\cap L}$, we have

$$Gal(KL|F) \subset H \ .$$

We have to prove that they are equal. This is because $\sigma|_{K\cap L} = \tau|_{K\cap L}$. So write an element of KL as

$$\prod_i a_i^{n_i} \prod_j b_j^{m_j}$$

define

$$\sigma'(\prod_i a_i^{n_i} \prod_j b_j^{m_j}) = \prod_i \sigma(a_i)^{n_i} \prod_j \tau(b_j)^{m_j}$$

this is well defined because $\sigma|_{K\cap L} = \tau|_{K\cap L}$. Also we have $\sigma'|_K = \sigma$ and $\sigma'|_L = \tau$. So H is precisely the image.

d)Suppose that the group $Gal(KL|F) \cong Gal(K|F) \times Gal(L|F)$. Then we have to prove that $K \cap L = F$. That would mean that the group generated by $Gal(K|F)$ and $Gal(L|F)$ is $Gal(KL|F)$. Since $Gal(KL|F)$ is isomorphic to $Gal(K|F) \times Gal(L|F)$. We have $Gal(K|F) \cap Gal(L|F) = \{0\}$, so by the Galois correspondence we have $K \cap L = F$.

On the other hand suppose $K \cap L = F$. Then it follows that $Gal(KL|F) \cong Gal(K|F) \times Gal(L|F)$ by the Galois correspondence.

Solution of problem 4

$K|F$ is a finite Galois extension. Let L be an intermediate subfield. Let $H = Gal(K|L)$. Let $N(H)$ be the normalizer of H in $Gal(K|F)$. L_0 be the fixed field of $N(H)$. We have to prove that L is Galois over L_0, that is we have to prove that H is normal in $N(H)$. But that is true by definition of $N(H)$. Suppose that $L|E$ is Galois. Then we have that H is contained in H_E, and H is normal in H_E, taht would mean that H_E is inside $N(H)$. So we have $L_0 \subset E$.

Solution of problem 5

a) The derivative of $x^{p^n} - x$ is

$$p^n x^{p^n - 1} - 1 = -1$$

so the gcd of the polynomial $x^{p^n} - x$ with its derivative is 1. Therefore $x^{p^n} - x$ has no repeated roots.

b)We have to prove that for all α such that

$$\alpha^p = \alpha$$

we have

$$\alpha^{p^n} = \alpha \ .$$

$$(\alpha^p)^p = \alpha^{p^2} =$$

on the other hand

$$(\alpha^p)^p = \alpha$$

so we get

$$\alpha^{p^2} = \alpha$$

so this way we get that

$$\alpha^{p^n} = \alpha \ .$$

c) Follows from the fact that

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta \ ,$$

and

$$(\alpha\beta)^{p^n} = \alpha^{p^n} \beta^{p^n} = \alpha\beta \ .$$

Therefore we get that

$$(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1} \ .$$

d) Since the polynomial $x^{p^n} - x$ has p^n roots we get that cardinality of $\mathbb{F}_{p^n}$ is p^n. Since $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is Galois and the Galois group has order n we have that the degree of extension of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is n.

Solution to problem 6

Let $K|F$ is a separable extension of degree p^2. Now degree of the minimal polynomial is equal to the degree of the extension $K = F(a)$ over F which is p^2. K contains more than p roots of the minimal polynomial $m_a(x)$, which is of degree p^2. Now m_a has p^2 distinct roots. Consider the splitting field L of $m_a(x)$, since $m_a(x)$ is separable we have that the splitting field of $m_a(x)$ is Galois and therefore $[L : F] = |Aut(L|F)| = p^2$, since we have p^2 many distinct roots. Since $|Aut(K|F)|$ divides the order of $Aut(L|F)$ and K contains more than p roots of the minimal polynomial we have that $Aut(K|F) = Aut(L|F)$, whence we get that $L = K$. So K is the splitting field of $m_a(x)$. So $K|F$ is normal. Therefore it is Galois and hence its Galois group is of order p^2. Since any group of order p^2 is abelian, we have only two possibilities $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.