Mat347 Tutorial 15

Separable and inseparable field extensions

The Frobenius map

4. Find a K such that σ_p is not onto.
Solution: Consider the field $F_p(t)$.
Claim: There is no $\frac{f}{g}$ such that $(\frac{f}{g})^p = t$.

Proof. $deg((\frac{f}{g})^p) = pdeg(f) - pdeg(g) = p(deg(f) - deg(g)) = 1$ This is impossible. Therefore, $\nexists \frac{f}{g} \in F_p(t)$ s.t. $\sigma_p(\frac{f}{g}) = t$ □

5. Let p be prime. Let $f(x) = x^p - t \in F_p(t)[x]$. Is f separable? Let K be a splitting field of f over $F_p(t)$. Describe $Aut(K/F_p(t))$.
Solution: $f'(x) = px^{p-1} = 0$. Then consider a root α such that $f(\alpha) = 0$. Then $f'(\alpha) = 0 \Rightarrow$ multiplicity of α is not one. Therefore, it is not separable.
Let K be a splitting field of f over $F_p(t)$. It's easy to see that K is not Galois over $F_p(t)$ since f is not separable. (Check proposition from book). Indeed, let α be the solution of $f(x)$, then $\alpha^p - t = 0 \Rightarrow t = \alpha^p \Rightarrow x^p - t = x^p - \alpha^p = (x - \alpha)^p$. Then by U.F.D we can see that α is the only solution of $x^p - t$. Then $K = F_p(t)(\alpha)$.
$\forall \sigma \in Aut(K/F_p(t))$, $\sigma(\alpha)$ is a root of $\sigma(f)(x) = f(x)$, and we just show $f(x)$ only has one root, thus $\sigma(\alpha) = \alpha$. Then $Aut(K/F_p(t)) = Aut(F_p(t)(\alpha)/F_p(t)) = 1$.
Claim: $x^p - t$ is irreducible

Proof. Suppose $x^p - t$ is reducible, then $x^p - t = f(x)g(x)$, in the splitting field, we know $x^p - t = (x - \alpha)^p$ for some α and a field is U.F.D, then we can say $f(x) = (x - \alpha)^r$ for some r such that $1 \leq r \leq p - 1$. Since $f(x) \in F_p(t)[x] \Rightarrow \alpha^r \in F_p(t)$. Then since $gcd(r, p) = 1$, $\exists x, y$ such that $rx + py = 1$. We have $\alpha^r \in F_p(t), \alpha^p \in F_p(t)$. Thus $\alpha^{rx}\alpha^{py} \in F_p(t) \Rightarrow \alpha^{rx+py} = \alpha \in F_p(t)$. Then this means $\exists \alpha \in F_p(t)$ such that $\alpha^p - t = 0$, contradicts the result that we get above. □

6. Prove that if $f \in K[x]$ then $f' = 0$ if and only if there exists $g \in K[x]$ such that $f(x) = g(x^p)$.

Proof. One direction is obvious.
Now suppose $f' = 0$, then assume $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

$$\Rightarrow na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 = 0$$
$$\Rightarrow n = pk, p \nmid n-1, n-2, \ldots, n-(p-1)$$
$$\Rightarrow a_{n-1}, a_{n-2}, \ldots, a_{n-(p-1)} = 0$$
$$\Rightarrow a_n, a_{n-p}, a_{n-2p}, \ldots, a_{n-(k-1)p} \neq 0$$
$$\Rightarrow f = a_n x^{pk} + a_{n-p}x^{p(k-1)} + a_{n-2p}x^{p(k-2)} + \cdots + a_p x^p + a_0$$
$$\Rightarrow f = g(x^p) \text{ for some g}$$

□

7. Prove that K is perfect if and only if $\sigma_p \in Aut(K)$ (that is, if every element of K is a p^{th} power in K).

   Proof. ($\Rightarrow$)
   K is perfect implies for any irreducible polynomial $f(x) \in K[x]$, $f(x)$ is separable. Thus $f' \neq 0$. Then consider $\alpha \in K$ then $(x^p - \alpha)' = 0 \Rightarrow x^p - \alpha$ is reducible. Then let β be the solution of $x^p - \alpha$, we will have $\beta^p = \alpha$. Then in the splitting field $K(\beta)$ we have $x^p - \alpha = x^p - \beta^p = (x-\beta)^p$. Thus let $x^p - \alpha = g_1(x)g_2(x)$ such that $g_1(x), g_2(x) \in K[x]$. Therefore, $g_1(x) = (x-\beta)^r$ for some r, by similar way as above proof, $\beta^r \in K$, $\beta^p \in K$, and $gcd(r,p) = 1$, thus $\beta \in K$. Therefore, this means $\forall \alpha \in K, \exists \beta \; s.t. \; \beta^p = \alpha \Rightarrow \sigma_p$ is a bijective homomorphism $K \to K$, thus $\sigma_p \in Aut(K)$

   ($\Leftarrow$)
   Suppose $\forall \alpha \in K, \exists \beta \; s.t. \; \beta^p = \alpha$. Then consider any irreducible function f. If $f' = 0$, by 6 we will have $f = g(x^p) = a_0 + a_1 x^p + a_2 x^{2p} + a_n x^{np}$, by assumption, $\exists \gamma_i \; s.t. \; \gamma_i^p = a_i$, we will have $f = \gamma_0^p + \gamma_1^p x^p + \gamma_2^p x^{2p} + \cdots + \gamma_n^p x^{np} = (\gamma_0 + \cdots + \gamma_n x^n)^p$. However this contradicts with $f(x)$ is irreducible, thus $f' \neq 0$. Therefore, $\forall f \in K[x], f' \neq 0$, K is perfect. □

8. Prove that every algebraic extension of F_p is perfect.

   Proof. From 3 and 7 we can see this easily. □

9. Prove that if a finite extension L of K is inseparable, then p divides $[L : K]$.

   Proof. Let α be the root of $m_{\alpha,K}(x)$ such that $m_{\alpha,K}(x)$ is not separable. Then $m_{\alpha,K}(x)' = 0$. Thus $m_{\alpha,K}(x) = g(x^p)$ for some $g(x)$ such that $g(x)$ is irreducible (otherwise $m_{\alpha,K}(x)$ is reducible). Then by definition $K(\alpha)$ is a subfield of L and $p \,|\, [K(\alpha) : K] \Rightarrow p \,|\, [L : k]$ □

10. Prove that if L is a finite purely inseparable extension of K, then $[L : K]$ is a power of p.

Proof. Claim: If $f(x)$ is irreducible inseparable, then $f(x) = g(x^{p^n})$ such that g is irreducible and separable.
The proof is almost same as q6 plus the induction on if g_i is separable.
Then with the claim above, let $\alpha \in L\backslash K$, $f(x) = m_{a,K}(x)$, we can show that $\exists$ irreducible separable

$$g(x) = \prod_{1 \le i \le m} (x - a_i)$$

(by g is separable),

$$f(x) = \prod_{1 \le i \le m} (x^{p^n} - a_i)$$

.
Now we want to show that $f(x) = (x^{p^n} - a)$ in other word $m = 1$.
Okay, let's prove this. First we can say $a_i \notin L\backslash K$. Otherwise $g(x)$ is the minimal polynomial of a_i, but $g(x)$ is separable, contradict with L is a finite purely inseparable extension of K. However, $f(\alpha) = 0 \Rightarrow \alpha^{p^n} = a_i$ for some i. And $\alpha \in L \Rightarrow \alpha^{p^n} \in L \Rightarrow a_i \in L \Rightarrow a_i \in K \Rightarrow f(x) = (x^{p^n} - a)$ $s.t.$ $a \in K$. Then for anyother $m_{\beta,K}(x)$, we could either show $\beta \in K(\alpha)$ or $m_{\beta,K}(x)$ is irreducible in $K(\alpha)$. Then we simply use the induction, completes the proof. $\square$