TOPICS IN THEORY OF FIELDS

1. Introduction

In this notes we discuss more advanced topics in theory of fields. Our main result is famous Mac Lane's characterization (Theorem 4.3) of infinite separable extensions. From this result we derive interesting characterization of perfect fields in Corollary 4.4 and geometrically reduced algebras in Proposition 4.6.

2. Separable degree

Definition 2.1. Suppose that $k \subseteq K$ is a finite extension of fields and $k \subseteq \overline{k}$ is an algebraic closure of k. The number of elements of the set

$$\{\sigma : K \to \overline{k} \mid \sigma \text{ is a } k\text{-morphism}\}$$

is denoted by $[K : k]_s$ and is called *the separable degree of the extension* $k \subseteq K$.

Fact 2.2. *Suppose that $k \subseteq K$ and $K \subseteq L$ are finite extensions of fields. Then $[L : k]_s = [L : K]_s \cdot [K : k]_s$.*

Proposition 2.3. *Suppose that k is a field and $f \in k[x]$ is an irreducible polynomial. Then*

$$f(x) = \begin{cases} \prod_{i=1}^{n}(x - a_i) & \textit{if } \mathrm{char}(k) = 0 \\ \prod_{i=1}^{n}(x - a_i)^{p^m} & \textit{if } \mathrm{char}(k) = p > 0 \end{cases}$$

for pairwise disjoint elements $a_1, ..., a_n$ of algebraic closure of k.

Proof. Fix an algebraic closure K of k. Observe that f has multiple roots if and only if f and $\frac{\partial f}{\partial x}$ have noninvertible common divisors in $K[x]$.
Suppose that $\mathrm{char}(k) = 0$. Then $\frac{\partial f}{\partial x} \neq 0$ and f cannot have multiple roots, since by irreducibility of f this would imply that $f \mid \frac{\partial f}{\partial x}$ in $k[x]$.
Assume now that $\mathrm{char}(k) = p > 0$. If f has multiple roots, then $f \mid \frac{\partial f}{\partial x}$ and hence $\frac{\partial f}{\partial x} = 0$. Thus $f(x) = h(x^p)$. Clearly h is irreducible over k. We can apply this argument again to h. Eventually we derive that $f = g(x^{p^m})$ for some positive $m \in \mathbb{N}$ and g is irreducible without multiple roots. Hence the result follows. □

Corollary 2.4. *Suppose that $k \subseteq K$ is a finite extension. Then $[K : k]_s \mid [K : k]$.*

Proof. This is a combination of Fact 2.2 and Proposition 2.3. □

Definition 2.5. Suppose that k is a field and f is an irreducible polynomial in $k[x]$. Then f is *separable* if and only if it has no multiple roots.

Definition 2.6. Suppose that $k \subseteq K$ is an extension of fields and a is an element of K algebraic over k. Then a is *separable* if and only if its minimal polynomial over k is separable.

Corollary 2.7. *Suppose that $k \subseteq K$ is a finite extension. Then the following assertions are equivalent.*

(i) *Every a in K is separable over k.*

(ii) *K is generated by elements separable over k.*

(iii) $[K : k]_s = [K : k]$

Theorem 2.8 (Abel's theorem)**.** *Suppose that $k \subseteq K$ is a finite extension of fields generated by separable elements. Then there exists an element a in K such that $K = k(a)$.*

Proof. This is clear for k finite.
Suppose that k is infinite. By easy induction we may assume that $K = k(b, c)$. Let $\sigma_1, ...\sigma_n$ be all distinct k-morphisms of K into some algebraic closure $\overline{k}$ of k. Then $n = [K : k]$ by Corollary 2.7. Consider the polynomial

$$f(x) = \prod_{1 \leq i < j \leq n} \Big(\big(\sigma_i(b) - \sigma_j(b)\big)x + \big(\sigma_i(c) - \sigma_j(c)\big) \Big)$$

Since k is infinite, we may assume that there exists $l \in k$ such that $f(l) \neq 0$. Then we have $\sigma_i(bl + c) \neq \sigma_j(bl + c)$ for all $i \neq j$. Hence

$$[k(bl + c) : k] \leq [K : k] = n = [k(bl + c) : k]_s \leq [k(bl + c) : k]$$

Thus $k(bl + c) = K$. □

Definition 2.9. Suppose that $k \subseteq K$ is a finite extension of fields. Then $[K : k]_i = \frac{[K:k]}{[K:k]_s}$ is called *inseparable degree*.

Corollary 2.10. *Suppose that $k \subseteq K$ is a finite extension of fields. Then $[K : k]_i$ is some power of* $\mathrm{char}(k)$.

Definition 2.11. A field k is *perfect* if for every finite algebraic extension $k \subseteq K$ every element of K is separable over k.

3. Purely inseparable extensions

Definition 3.1. Let $k \subseteq K$ be a fields extension. We say that it is *purely inseparable* if for every extension of fields $k \subseteq L$ ring $K \otimes_k L$ has the unique prime ideal.

Proposition 3.2. *Suppose that $k \subseteq K$ is an extension of fields. Then the following assertions are equivalent.*

- **(i)** *$k \subseteq K$ is purely inseparable.*
- **(ii)** *For every fields extension $k \subseteq L$ there exists at most one morphism $K \to L$ over k.*
- **(iii)** $\mathrm{char}(k) = p > 0$ *and for every a in K element a^{p^n} is in k for some $n \in \mathbb{N}$.*

Proof. Suppose that $k \subseteq K$ is purely inseparable and assume that $f, g : K \to L$ are k-morphisms. Let $\overline{f} : K \otimes_k L \to L$ and $\overline{g} : K \otimes_k L \to L$ be morphisms given by $\overline{f}(x \otimes y) = f(x) \cdot y$ and $\overline{g}(x \otimes y) = g(x) \cdot y$. Then $\overline{f}$ and $\overline{g}$ are surjective morphisms of L-algebras. Since $K \otimes_k L$ has the unique prime ideal, we have that $\overline{f} = \overline{g}$. Therefore, $f(x) = \overline{f}(x \otimes 1) = \overline{g}(x \otimes 1) = g(x)$.
Suppose that the second assertion holds. Then clearly $k \subseteq K$ is algebraic. Suppose that there exists $a \in K \smallsetminus k$ that is separable over k. Then $k \to k(a)$ have at least two distinct k-morphisms to $\overline{k}$. Thus K has at least two distinct k-morphisms to $\overline{k}$. Therefore, there is no $a \in K \smallsetminus k$ that is separable. This shows that $\mathrm{char}(k) = p > 0$ and for any element $a \in K$ its minimal polynomial over k is of the form $x^{p^n} - a^{p^n}$.
Suppose now that the third assertion holds. Fix an extension $k \to L$ of fields. Then we have an integral extension of rings $L \to K \otimes_k L$ such that, for every x in $K \otimes_k L$ we have $x^{p^n} \in L$. Hence $K \otimes_k L$ has the unique prime ideal. □

4. Separable extensions

Definition 4.1. Suppose that $k \subseteq K$ is an extension of fields. If for every extension $k \subseteq L$ of fields ring $K \otimes_k L$ is reduced, then $k \subseteq K$ *is a separable extension*.

Definition 4.2. Suppose that $k \subseteq K$ is an extension of fields. A set of elements $\{x_i\}_{i\in I}$ of K is *a separating transcendence base of K over k* if it is a transcendence base of K over k and $k(\{x_i\}_{i\in I}) \subseteq K$ is an algebraic extension generated by separable elements.

Theorem 4.3 (Mac Lane's characterization)**.** *Let k be a field of characteristic $p > 0$ and $k \subseteq K$ be an extension of fields. Then the following assertions are equivalent.*

- **(i)** *$k \subseteq K$ is separable.*
- **(ii)** *$K \otimes_k k^{\frac{1}{p^\infty}}$ is reduced.*
- **(iii)** *$K \otimes_k k^{\frac{1}{p}}$ is reduced.*
- **(iv)** *Every finite set $x_1, ...x_n \in K$ contains a separating transcendence base of $k(x_1, ..., x_n)$ over k.*

Proof. The only nontrivial implications are **(iii)** $\Rightarrow$ **(iv)** and **(iv)** $\Rightarrow$ **(i)**.
Suppose that the third assertion hold. Since $k \subseteq k^{\frac{1}{p}}$ is purely inseparable and $K \otimes_k k^{\frac{1}{p}}$ is reduced, we derive by Proposition 3.2 that $K \otimes_k k^{\frac{1}{p}}$ is a field. Fix algebraically closed field L containing K and consider a monomorphism $K \otimes_k k^{\frac{1}{p}} \to L$. Its image is a subfield of L isomorphic with $K \otimes_k k^{\frac{1}{p}}$. We denote it by $Kk^{\frac{1}{p}}$. Assume that $k(x_1, ..., x_s) \subseteq K$ and $\mathrm{tr}_k k(x_1, ..., x_s) = s - 1$. Suppose that $f(t_1, ..., t_s) \in k[t_1, ..., t_s]$ is a nonzero polynomial such that

$$f(x_1, ..., x_s) = 0$$

Moreover, we may assume that f is of the smallest total degree among such polynomials in $k[t_1, ..., t_s]$. Write

$$f(t) = \sum_{\alpha\in\mathbb{N}^s} c_\alpha M_\alpha(t)$$

where $M_\alpha(t) = t_1^{\alpha_1} ...t_s^{\alpha_s}$ and $\alpha = (\alpha_1, ..., \alpha_s)$. Let $M_\alpha(x)$ be an evaluation of $M_\alpha(t)$ in $(x_1, ..., x_s)$. If $p \mid \alpha$ for every $\alpha \in \mathbb{N}^s$ such that $c_\alpha \neq 0$, then $f = g^p$ for some polynomial $g \in k^{\frac{1}{p}}[t_1, ..., t_s]$. In this case

$$0 = f(x_1, ..., x_s) = g(x_1, ..., x_s)^p$$

and $g(x_1, ..., x_s) \in Kk^{\frac{1}{p}}$. Moreover, elements $M_{\frac{\alpha}{p}}(x)$ for $c_\alpha \neq 0$ are linearly indepedent over k, since their linear dependence will lead to contradiction with the fact that f is of the smallest total degree. Since $k(x_1, ..., x_s) \otimes_k k^{\frac{1}{p}} \to Kk^{\frac{1}{p}}$ is a monomorphism, we derive that elements $M_{\frac{\alpha}{p}}(x)$ for $c_\alpha \neq 0$ are linearly indepedent over $k^{\frac{1}{p}}$. Thus $g(x_1, ..., x_s) \neq 0$, which leads to a contradiction with the fact that $g(x_1, ..., x_s)^p = 0$. Therefore, there exists $\gamma \in \mathbb{N}^s$ such that, $c_\gamma \neq 0$ and $p \nmid \gamma$. There exists $r \in \{1, ..., s\}$ such that $p \nmid \gamma_r$. Thus by minimality assumption on f and Proposition 2.3 we can interpreted $f(x_1, ..., x_s) = 0$ as an irreducible algebraic relation of x_r over $k(x_1, ..., x_{r-1}, x_{r+1}, ..., x_s)$ in such a way that x_r becomes separable over $k(x_1, ..., x_{r-1}, x_{r+1}, ..., x_s)$. Now the general case of **(iv)** follows by easy induction.
Suppose now that **(iv)** holds. Fix a field extension $k \subseteq L$. Pick any finite set of elements $x_1, ...x_n \in K$. We may assume that $x_1, ..., x_m$ for some $m \leq n$ form a separating transcendence base of $k(x_1, ..., x_n)$ over k. Then

$$k(x_1, ..., x_n) \otimes_k L \cong k(x_1, ..., x_n) \otimes_{k(x_1,...,x_m)} (k(x_1, ..., x_m) \otimes_k L) \subseteq k(x_1, ..., x_n) \otimes_{k(x_1,...,x_m)} L(x_1, ..., x_m)$$

is reduced by Theorem 2.8. Thus $K \otimes_k L$ is reduced, since K is a colimit of finitely generated extensions. $\square$

Corollary 4.4. *Suppose that k is a field. Then the following assertions are equivalent.*

(i) *Every extension $k \subseteq K$ is separable.*

(ii) $k = k^{\frac{1}{p^\infty}}$

(iii) *k is perfect.*

Definition 4.5. Let A be an algebra over a field k. Suppose that for every reduced k-algebra B tensor product $A \otimes_k B$ is reduced. Then A is *geometrically reduced*.

Proposition 4.6. *Let A be an algebra over a field k. Then the following assertions are equivalent.*

(i) *A is a geometrically reduced k-algebra.*

(ii) *$A \otimes_k \overline{k}$ is reduced.*

(iii) *$A \otimes_k k^{\frac{1}{p^\infty}}$ is reduced.*

Proof. We show that **(iii)** $\Rightarrow$ **(i)**. First let us make two general remarks.
Suppose that A and B are some k-algebras, B is reduced and we want to show that $A \otimes_k B$ is reduced. Since every k-algebra is a colimit of its finitely generated subalgebras, we may assume that B is a finitely generated and reduced k-algebra. Next, using the fact that noetherian ring has finitely many minimal primes, we may assume that B is a product of finitely many domains. Finally each domain can be embedded into its field of fractions. Thus we may assume that B is a field over k.
Secondly observe that if $k \subseteq L$ is a separable extension, then L is geometrically reduced over k. This follows easily from what we have said above.
Now we can prove the implication. By the first remark it suffices to show that $A \otimes_k L$ is reduced for every extension $k \subseteq L$ of fields. Obviously we may assume that L contains $k^{\frac{1}{p^\infty}}$. Since the field $k^{\frac{1}{p^\infty}}$ is perfect, the extension $k^{\frac{1}{p^\infty}} \subseteq L$ is separable. By the second remark, L is geometrically reduced over $k^{\frac{1}{p^\infty}}$. Now observe that

$$A \otimes_k L \cong (A \otimes_k k^{\frac{1}{p^\infty}}) \otimes_{k^{\frac{1}{p^\infty}}} L$$

is reduced, since $A \otimes_k k^{\frac{1}{p^\infty}}$ is reduced and $k^{\frac{1}{p^\infty}} \subseteq L$ is geometrically reduced. This completes the proof of the implication.
The implications **(i)** $\Rightarrow$ **(ii)** and **(ii)** $\Rightarrow$ **(iii)** are immediate. $\square$