Chapter5 Fields and Galois theory Solutions

October 5, 2020

Field Extensions

1.

(a) $[F : K] = 1$ if and only if $F = K$.
(b) If $[F : K]$ is a prime, then there are no intermediate fields between F and K
(c) If $u \in F$ has degree n over K, then n divides $[F : K]$

Proof. (a) $\Rightarrow$: If $[F : K] = 1$ then let $\{u\}, u \in F$ be the basis of F. If $u = 0$ then $F = 0$ as every elements in F has the form ku for some $k \in K$.Let f be a map, which is $f : K \to F, k \mapsto ku$. Then it's easy to see that f is injective. By the fact that every element in F has form ku for some $k \in K$, we have f is surjective, hence f is bijective. Therefore $F = K$.

$\Leftarrow$ If $F = K$ then any nonzero element could be the basis of F over K
(b)If there is some intermediate field E between F and K then we have

$$[F : K] = [F : E][E : K]$$

which means $[F : E] = 1$ or $[E : K]$=1 as $[F : K]$ is prime. Therefore we have $F = E$ or $E = K$ by (a).
(c) By the condition, let f be the minimal polynomial of u over K, we have that $1, u, u^2, ..., u^{n-1}$ is a basis of $K(u)$(**Theorem1.6**) Notice that $K(u)$ is an intermediate field between K and F, we have n divides $[F : K]$ by **Theorem1.2**

2.

Give an example of a finitely generation field extension, which is not finite dimensional.

Solution. Consider $\mathbb{Q}(e)$, it's obvious that $\mathbb{Q}(e)$ is a finitly generated extension but $\mathbb{Q}(e)$ is not finite dimensional over $\mathbb{Q}$, otherwise e is algebraic over $\mathbb{Q}$, which is false.

3.

If $u_1, u_2, ..., u_n \in F$ then the field $F(u_1, ..., u_n)$ is isomorphic to the quotient field of the ring $K[u_1, ..., u_n]$.

Proof. Define map between $F(u_1, ..., u_2)$ and the quotient field of $F[u_1, ..., u_n]$ as follows:

$$f : h(u_1, ..., u_n)/k(u_1, ..., u_n) \mapsto (h(u_1, ..., u_n), k(u_1, ..., u_n))$$

It's easy to see that f is an isomorphism.

4.

(a) For any $u_1, ..., u_n \in F$ and any permutation $\sigma \in S_n, K(u_1, ..., u_n) = K(u_{\sigma(1)}, ..., u_{\sigma(n)})$
(b) $K(u_1, ..., u_{n-1})(u_n) = K(u_1, ..., u_{n-1}, u_n)$
(c) State and prove the analogues of (a) and (b) for $K[u_1, ..., u_n]$.
(d) If each u_i is algebraic over K, then $K(u_1, ..., u_n) = K[u_1, ..., u_n]$

Proof. (a) According to the definition and remark after **Theorem1.2**, $K(u_1, ..., u_n)$ is the subfield generated by $F \cup \{u_1, ..., u_n\}$ and $K(u_{\sigma(1)}, ..., u_{\sigma(n)})$ is the subfield generated by $F \cup \{u_{\sigma(1)}, ..., u_{\sigma(n)}\}$. These two sets are equal as σ is bijective.

(b)$K(u_1, ..., u_{n-1})(u_n)$ is a subfield (of F) that contains $u_1, .., u_{n-1}, u_n$, therefore according to the difinition of $K(u_1, ..., u_n)$, we have:

$$K(u_1, ..., u_n) \subset K(u_1, ..., u_{n-1})(u_n)$$

On the other hand, $K(u_1, ..., u_{n-1})(u_n)$ is the subfield generated by $K(u_1, ..., u_{n-1}) \cup \{u_n\}$ Notice that $K(u_1, ..., u_n)$ contains $K(u_1, ..., u_{n-1})$ and u_n, we have:

$$K(u_1, ..., u_{n-1})(u_n) \subset K(u_1, ..., u_n)$$

therefore these two subfield are equal.

(c) The analogues of $K[u_1, ..., u_n]$ are easy to write and prove as long as we replace "subfield" with "subring".

(d) We prove by induction: when $n = 1$ this holds as $K(u) = K[u]$, which is showed in **Theorem1.6**. Let's assume $K(u_1, ..., u_{n-1}) = K[u_1, ..., u_{n-1}]$, then u_n is algebraic over K implies u_n is also algebraic over $K(u_1, ..., u_{n-1})$. We have:

$$K(u_1, ..., u_n) = K(u_1, ..., u_{n-1})(u_n) = K[u_1, ..., u_{n-1}](u_n) = K[u_1, ..., u_{n-1}][u_n] = K[u_1, ..., u_n]$$

The count-down-2 equation follows from the conclusion of adding one algebraic element.

5.

Let L and M be subfields of F and LM their composite.
(a) If $K \subset L \cap M$ and $M = K(S)$ for some $S \subset M$, then $LM = L(S)$.
(b) When is it true that LM is the set theoretic union $L \cup M$
(c) If $E_1, ..., E_n$ are subfields of F, show that

$$E_1 E_2 ... E_n = E_1(E_2(...(E_{n-1}(E_n))...)).$$

Proof. PASS

6.

Every element of $K(x_1, ..., x_n)$ which is not in K is transcendental over K.

Proof. PASS: I feel this question is incorrect

7.

If v is algebraic over $K(u)$ for some $u \in F$ and v is transcendental over K, then u is algebraic over $K(v)$.

Proof. v is algebraic over $K(u)$ means there is some polynomial $f \in K(u)[x]$ such that $f(u) = 0$. We can write this in the following form:

$$\sum_{i=0}^{n} \frac{h_i(u)}{k_i(u)} v^i = 0, h_i(x), k_i(x) \in K[x]$$

. By multiplying $\prod_{i=0}^{n} h_i(u)$ we have:

$$\sum_{i=0}^{n} F_i(u) v^i = 0, F_i(u) = \prod_{j \neq i} k_j(u) h_i(u)$$

If we combine all coefficiences of each u^i together, we will have:

$$\sum_{i=0}^{m} G_i(v) u^i = 0, G_i(x) \in K[x]$$

Notice that $G_i(v) \neq 0, \forall i = 0, ..., m$ as v is transcendental over K. We have u is algebraic over $K(v)$.

8.

If $u \in F$ is algebraic of odd degree over K, then so is u^2 and $K(u) = K(u^2)$

Proof. If u is algebraic over K then $[F(u) : F]$ is finite and equals to the degree of the minimal polynomial of u. It's easy to see that $K(u^2)$ is an intermediate between K and $K(u)$, according to **Theorem1.2** we have $[K(u^2) : K] \mid [K(u) : K]$. Now that $[K(u) : K]$ is odd, so is $[K(u^2) : K]$ and u^2 has odd degree, which shows u^2 is also algebraic over K

Let $f(x) = \sum_{i=0}^{p} k_i x^i$ be the minimal polynomial of u over K, then we have: $\sum_{i=0}^{p} k_i u^i = 0$. Do the following transmission:

$$u \sum_{i \text{ is odd}} k_i (u^2)^{\frac{i-1}{2}} + \sum_{i \text{ is even}} k_i (u^2)^{\frac{i}{2}} = 0$$

Let $h(x) = \sum_{i \text{ is odd}} k_i x^{\frac{i-1}{2}}, g(x) = \sum_{i \text{ is even}} k_i x^{\frac{i}{2}}$ Then we have: $u = -\frac{g(u^2)}{h(u^2)}$($p$ is odd guarrantees $h(x)$ exists and not equals to 0, the minimal of p guarrantees $h(u) \neq 0$),

Therefore we have $u \in K(u^2)$, hence $K(u) \subset K(u^2)$. It's obvious that $K(u^2) \subset K(u)$, then we have $K(u^2) = K(u)$

9.

If $x^n - a \in K[x]$ is irreducible and $u \in F$ is a root of $x^n - a$ and m divides n, then prove that the degree of u^m over K is n/m. What is the irreducible polynomial for u^m over K?

Proof. u is a root of $f(x) = x^n - a$ means $u^n - a = 0$, we have $(u^m)^{\frac{n}{m}} - a = 0$ Let $g(x) = x^{\frac{n}{m}} - a$, we claim that $g(x)$ is the minimal polynomial of u^m.

If there is another $g^{'}(x)$ such that $\deg g^{'} < \deg g$ and $g^{'}(u^m) = 0$. Then there is a polynomial $f^{'}(x)$ with degree of $\deg g^{'} \times m$, which is less that $\deg f$ such that $f^{'}(u) = 0$, which contradicts the defintion of minimal polynomial. Therefore we hace degree of u^m over K is $\frac{n}{m}$

The fact that there is only one minimal polynomial(let f, g be minimal polynomials, then $f \mid g$ and $g \mid f$) shows that $x^{\frac{n}{m}} - a$ is the minimal polynomial of u^m

10.

If F is algebraic over K and D is an integral domain such that $K \subset D \subset F$,then D is a field

Proof. For any element $d \in D \subset F$, consider $d^{-1} \in F$. Let $f(x)$ be the minimal polynomial of d^{-1} over K(F is algebraic over K by condition) Then we have: $f(d^{-1}) = 0$, write it as :

$$\sum_{i=0}^{n} k_i d^{-i} = 0 \Rightarrow d^{-1} = (k_n)^{-1} d^{n-1} \sum_{i=0}^{n-1} k_i d^{-i} = (k_n)^{-1} \sum_{i=0}^{n-1} k_i d^{n-1-i}$$

Therefore $d^{-1} \in D$ and D is a subgroup of F under multiplication

12.

If $d \geq 0$ is an integer that is not a square describe the field $\mathbb{Q}(\sqrt{d})$ and find a set of elements that generate the whole field.

Solution. PASS: I don't understand what it means.

13.

(a) Consider the extension $\mathbb{Q}(u)$ of $\mathbb{Q}$ generated by a real root u of $x^3 - 6x^2 + 9x + 3$.(Why is this irreducible?) Express each of the following elements in terms of the basis $\{1, u, u^2\}$:$u^4, u^5, 3u^5 - u^4 + 2; (u+1)^{-1}; (u^2 - 6u + 8)^{-1}$.
(b) Do the same with respect to the basis $\{1, u, u^2, u^3, u^4\}$ of $\mathbb{Q}(u)$ where u is a real root of $x^5 + 2x + 2$ and the elements in question are: $(u^2+2)(u^3+3u); u^{-1}; u^4(u^4+3u^2+7u+5); (u+2)(u^2+3)^{-1}$

Solution. (a) $u^4 = 27u^2 - 57u - 18$, $u^5 = 105u^2 - 261u - 81$.
By using Euclidean Algorithm, we calculated that $\gcd(x^3 - 6x^2 + 9x + 3, x + 1) = 1$ and:

$$-(x^3 - 6x^2 + 9x + 3) + (x+1) \times \frac{1}{14}(x^2 - 8x + 17) = 1$$

Therefore $(u+1)^{-1} = \frac{1}{14}(u^2 - 8u + 17)$.
(b) The same as (a), but there are more calculations

14.

(a) If $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$,find $[F : \mathbb{Q}]$ and a basis of F over $\mathbb{Q}$.
(b) Do the same for $F = \mathbb{Q}(i, \sqrt{3}, \omega)$,where $i \in \mathbb{C}, i^2 = -1$,and ω is a complex (nonreal) cube root of 1.

Solution. (a) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \times [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ It's easy to see that these two components are both 2, hence we have : $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.The basis are $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.
(b) Notice that $\omega = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i$, we have: $\omega \in \mathbb{Q}(i, \sqrt{3})$. Then we have:$[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}(i)] \times [\mathbb{Q}(i) : \mathbb{Q}]$, which equals to $2 \times 2 = 4$. The basis is $\{1, i, \sqrt{3}, \sqrt{3}i\}$

15.

In the field $K(x)$, let $u = x^3/(x + 1)$. Show that $K(x)$ is a simple extension of the field $K(u)$. What is $[K(x) : K(u)]$

Proof. Let $v = x^2/(x + 1)$, we will show that $K(u)(v) = K(x)$, which means $K(x)$ is simple extension of $K(u)$. $K(u)(v) \subset K(x)$ is obvious. Notice that $x = (x^3/(x + 1))/(x^2/(x+1)) = u/v$ We have:$x \in K(u)(v)$, moreover, any $f/g \in K(x)$ could be written as the combination of x^i, thus an element of $K(u)(v)$. Therefore we have $K(x) \subset K(u)(v)$ and $K(u)(v) = K(x)$.

16.

In the field $\mathbb{C}$, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic as vector spaces, but not as fields.

Proof. i and $\sqrt{2}$ is algebraic over $\mathbb{Q}$, thus by **Theorem1.6** we have:

$$\mathbb{Q}(i) = \mathbb{Q}[i] = \{f(i) \mid f(x) \in \mathbb{Q}[x]\} = \{a + bi \mid a, b \in \mathbb{Q}\}$$
$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{f(i) \mid f(x) \in \mathbb{Q}[x]\} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

Consider $\mathbb{Q}$-module homorphism:

$$f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(i) : a + b\sqrt{2} \mapsto a + bi$$

Then f is easy to be seen as $\mathbb{Q}$-module isomorphism, thus a vector space isomorphism. We will show that there is no filed-isomorphism between $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$. If there is some field-isomorphism f between these two fields of $\mathbb{C}$. Then we have:

$$f(a + bi) = f(a) + f(b)f(i), \forall a, b \in \mathbb{Q}$$

Then we have:

$$\begin{aligned} f(a)^2 + f(b)^2 = f(a^2 + b^2) &= f((a + bi)(a - bi)) = f(a + bi)f(a - bi) \\ &= (f(a) + f(b)f(i))(f(a) - f(b)f(i)) = f(a)^2 - f(b)^2 f(i)^2 \end{aligned}$$

This means $f(i)^2 = -1$ which is impossible in $\mathbb{Q}(\sqrt{2})$

REMARK. $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ as vector space is isomorphic is because they have the same dimension. And the difference between vector space and fields($mathbbQ(\sqrt{2})$ and $\mathbb{Q}(i)$ is that $f((a + bi)(a - bi)) = f(a + bi)f(a - bi)$ is not always true in vector space.

18.

A complex number is said to be an **algebraic number** if it is algebraic over $\mathbb{Q}$ and an **algebraic integer** if it is the root of a monic polynomial in $\mathbb{Z}[x]$.

(a) If u is an algebraic number, there exists an integer n such that nu is an algebraic integer.

(b) If $r \in \mathbb{Q}$ is an algebraic integer, then $r \in \mathbb{Z}$.

(c) If u is an algebraic integer and $n \in \mathbb{Z}$ then $u + n$ and nu are algebraic integers

(d) The sum and product of two algebraic integers are algebraic integers.

Proof. **(a)** If u is an algebraic number, let $f(x) \in \mathbb{Q}[x]$ satisfies $f(u) = 0$, and write $f(u)$ as the following form:

$$\sum_{i=0}^{n} \frac{p_i}{q_i} u^i = 0, p_i, q_i \in \mathbb{Z}$$

By multiplying the production of all q_i we can write this as:

$$\sum_{i=0}^{n} a_i u^i = 0, a_i \in \mathbb{Z}$$

. Multiplying a_n^{n-1} and we have: $\displaystyle\sum_{i=0}^{n} a_n^{n-1} a_i u^i = 0$, which is

$$\sum_{i=0}^{n} a_i a_n^{n-1-i} (a_n u)^i = 0$$

. Let $g(x) = \displaystyle\sum_{i=0}^{n} a_i a_n^{n-1-i} x^i$ then $g(x)$ is obvious monic and $g(a_n u) = 0$. Therefore $a_n u$ is an algebraic integer.

(b) Let $u = p/q$ with p and q $(p, q \in \mathbb{Z})$ relatively prime(absolute value) be an algebraic integer. And let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $f(u) = 0$, and write it as follows:

$$\sum_{i=0}^{n} a_i (\frac{p}{q})^i = 0, a_i \in \mathbb{Q}, a_n = 1$$

, multiplying q^n we will get:$\displaystyle\sum_{i=0}^{n} a_i p^i q^{n-i} = 0$ and $p^n = -q \displaystyle\sum_{i=0}^{n-1} a_i p^i q^{n-1-i}$. This implies that $q \mid p^n$ and thus $q \mid p$ as a result of p and q are relatively prime. We have $u = p/q$ is an integer.

(c) We first prove that $u + n$ is an algeraic integer, $\forall n \in \mathbb{Z}$. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $f(u) = 0$, written in the following form:

$$\sum_{i=0}^{m} a_i u^i = 0, a_i \in \mathbb{Z}, a_n = 1;$$

We have:$(u + n)^m + \displaystyle\sum_{i=1}^{m} (a_{m-i} - \binom{m}{i} n^i) u^{m-i} = 0$. By writing u^{m-1} in the above form and replace it with $(u + n)^{m-1}$, we will have:

$$(u + n)^m + (a_{m-1} - \binom{m}{1} n)(u + n)^{m-1} + \sum_{i=0}^{m-2} C_i u^i = 0$$

this process will continue to u and left a single term r in $\mathbb{Z}$. The polynomial: $g(x) = x^m + (a_{m-1} - \binom{m}{1})x^{m-1} + ... + r \in \mathbb{Z}[x]$ satisfies $g(u+n) = 0$ and $g(x)$ is monic. We draw the conclusion that $u+n$ is an algeraic integer.
As for nu, it's obvious if we multiply n^m in the equation: $\sum_{i=0}^{m} a_i u^i = 0$ and allocate each term $a_i u^i$ with n^i multiplying into u^i.

(d)