NAP 2019, MODULE II, HOMEWORK ASSIGNMENT #1

Michel Waldschmidt

Homework assignment, May 28, 2019.

• Problem 4.1 p. 42.

Assume $[L:K]$ is prime. If E is an extension of K contained in L, then the tower law yields $[L:K]=[L:E][E:K]$, hence
— either $[L:E]=1$, which means $E=L$,
— or else $[E:K]=1$, which means $E=K$.
Hence the intermediate fields are only L and K.

• Problem 4.2 p. 45.

If one of the two extensions $K_1:K$, $K_2:K$ is not finite, then $K(K_1,K_2):K$ is not a finite extension, and the result is true.

Assume now that both $K_1:K$ and $K_2:K$ are finite. In this case $K(K_1,K_2):K$ is a finite extension. Replacing L by $K(K_1,K_2)$, there is no loss of generality to assume that $L:K$ is a finite extension, hence an algebraic extension.

(a) To start with, let us show that if $L:K$ is an algebraic extension and A a subset of L which is a ring and a K–vector space, then A is a subfield of L. We need to prove that any nonzero element t in A has its inverse $1/t$ in A. By assumption t is algebraic over K. Let $a_0+a_1t+\cdots+a_nt^n=0$ be a polynomial relation for t with $a_j\in K$ and $a_0\neq 0$. Then

$$t^{-1}=-(a_1/a_0)-(a_2/a_0)t-\cdots-(a_n/a_0)t^{n-1}$$

and the assumptions imply that the right hand side is in A.

(b) Consider the subset A of L of finite sums $x_1y_1+\cdots+x_my_m$ where $x_i\in K_1$ and $y_i\in K_2$.

The sum and the product of two elements in A is again in A, hence A is a subring of L.

The product of an element of A by an element of K is in A, hence A is a subspace of the K–vector space L.

(c) Let $e_1,\dots,e_d$ be a basis of K_1 as a K–vector space and $f_1,\dots,f_m$ a basis of K_2 as a K–vector space. Then $d=[K_1:K]$, $m=[K_2:K]$ and any element in A is a finite sum of $a_{ij}e_if_j$, hence $\{e_if_j \mid 1\le i\le d,\ 1\le j\le m\}$ is a generating subset of A as a K–vector space. This shows that the dimension of A over K is $\le [K_1:K][K_2:K]$.

(d) Using (a), it follows that the field $K(K_1,K_2)$ is A, hence this field is an extension of K of degree $\le [K_1:K][K_2:K]$.

• Problem 4.3 p. 45.

Let $F(x)=\det(xI-T_\alpha)$ be the characteristic polynomial of T_α. By the Cayley–Hamilton Theorem, $F(T_\alpha)=0$. Since $T_\alpha^m=T_{\alpha^m}$ is the multiplication by α^m, the endomorphism $F(T_\alpha)$ of $K(\alpha)$ is the multiplication by $F(\alpha)$. Hence $F(\alpha)=0$. Now $F(x)$ is a monic polynomial in $K[x]$ of degree $[K(\alpha):K]$. Hence it is the minimal polynomial of α over K.

Here is another proof. Let $f(x)=x^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0$ be the minimal polynomial of α over K. A basis of $K(\alpha)$ over K is $(1,\alpha,\dots,\alpha^{d-1})$. For $0\le j<d-1$, we have $T_\alpha(\alpha^j)=\alpha^{j+1}$, while for $j=d-1$ we have

$$T_\alpha(\alpha^{d-1})=\alpha^d=-a_0-a_1\alpha-\cdots-a_{d-1}\alpha^{d-1}.$$

This means that in this basis, the matrix of T_α is

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{d-2} & -a_{d-1} \end{pmatrix}$$

The characteristic polynomial of this matrix is $f(x)$.

- Problem 4.4 p. 45.

A polynomial of degree 3 is irreducible over a field K if and only if it has no root in K[1].

The roots p/q in $\mathbb{Q}$, with $\gcd(x, y) = 1$, of a polynomial

$$a_d x^d + a_{d-1}x^{d-1} \cdots + a_1 x + a_0$$

with coefficients $a_i \in \mathbb{Z}$ and $a_0 a_d \neq 0$, have the property that a_0 divides p and a_d divides q. In particular when $a_0 = \pm 1$ and $a_d = \pm 1$ the only possible roots are 1 and -1. Here neither 1 not -1 is root of $x^3 + 3x + 1$, hence this polynomial is irreducible over $\mathbb{Q}$.

We have $\alpha^3 = -3\alpha - 1$, $\alpha^{-1} = -\alpha^2 - 3$.

There are several ways of finding the answer for $(1 + \alpha)^{-1}$, namely

$$(1 + \alpha)^{-1} = \frac{1}{3}\alpha^2 - \frac{1}{3}\alpha + \frac{4}{3}.$$

One solution is to write

$$(1 + \alpha)^{-1} = a_2\alpha^2 + a_1\alpha + a_0,$$

namely $(a_2\alpha^2 + a_1\alpha + a_0)(1 + \alpha) = 1$, to develop using $\alpha^3 = -3\alpha - 1$ and to solve the system of three equations in three unknowns

$$\begin{cases} a_1 + a_2 &= 0, \\ a_0 + a_1 - 3a_2 &= 0, \\ a_0 \qquad - a_2 &= 1. \end{cases}$$

Another solution is to write the Euclidean division in $\mathbb{Q}[x]$ of the polynomial $x^3 + 3x + 1$ by $x + 1$:

$$x^3 + 3x + 1 = (x + 1)(x^2 - x + 4) - 3$$

and to evaluate at $x = \alpha$:

$$0 = (\alpha + 1)(\alpha^2 - \alpha + 4) - 3.$$

- Problem 4.5 p. 45.

Let j be a complex root of $x^2 + x + 1$ (notice that $j^3 = 1$ and $j \neq 1$), let $\alpha = j + \sqrt[3]{2}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(j)$, $E = \mathbb{Q}(\sqrt[3]{2})$. We have $[E : \mathbb{Q}] = 3$, $[L : \mathbb{Q}] = 2$. It follows that $L(j) = E(\sqrt[3]{2}) = \mathbb{Q}(\alpha)$ is the field $\mathbb{Q}(E, L)$. From Problem 4.2 we deduce that it has degree ≤ 6 over $\mathbb{Q}$. Since it contains a subfield of degree 2 and a subfield of degree 3 over $\mathbb{Q}$, it has degree 6 over $\mathbb{Q}$. Notice that $[L(\alpha) : L] = 2$ and $[L : K] = 3$ are relatively prime.

The minimal polynomial of α over L is

$$(x - j)^3 - 2 = x^3 - jx^2 + j^2 x - 3$$

(with $j^2 = -j - 1$), its coefficients are not in K.

[1] This is true also for polynomials of degree 2, but not for polynomials of higher degree.

- Problem 4.6 p. 45.

  Since $[L : K] \neq 1$, we have $L \neq K$. Let $\alpha \in L \setminus K$. The field $K(\alpha)$ is a subfield of L containing K, it is not K, hence it is L (Problem 4.1).

- Problem 4.7 p. 47.

  Since K is countable, the set of polynomials with coefficients in K is also countable, hence the set of irreducible polynomials in $K[x]$ is countable, and each of them has only finitely many roots. Any element in L is a root of an irreducible polynomial with coefficients in K, hence L is countable.

  Since $\mathbb{Q}$ is countable, the set $\overline{\mathbb{Q}}$ of algebraic numbers is also countable. Since $\mathbb{R}$ is not countable, the set of transcendental numbers is not countable. In particular it is not empty.

- Problem 4.8 p. 47.

  (a) Write $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $d \geq 1$, $a_i \in K$ and $a_d \neq 0$. Since α is transcendental, it makes sense to say that the degree of $f(\alpha)$ in α is d. For $m \geq 1$ the degree in α of $f(\alpha)^m$ is md. Therefore the elements $1, f(\alpha), f(\alpha)^2, \dots, f(\alpha)^m, \dots$ are linearly independent (they have distinct degrees). This means that $f(\alpha)$ is transcendental over K.
  Remark. This shows that when α is transcendental over K, the only elements in $K[\alpha]$ which are algebraic over K are the elements in K. For solving Problem 4.10 below, we will need to prove more: the only elements in $K(\alpha)$ which are algebraic over K are the elements in K.

  (b) If β is algebraic over K, for $f \in K[x]$ we have $f(\beta) \in K(\beta)$, and $K(\beta)$ is an algebraic extension of K, therefore in this case $f(\beta)$ is algebraic over K. Hence if $f(\beta)$ is transcendental over K then β is transcendental over K.

- Problem 4.9 p. 48.

  The answer is no in general. For instance, since the set of $2^t = e^{t\log 2}$, $t \in \mathbb{R}$, t transcendental, is not countable, it contains transcendental numbers, and then the numbers $a = 2^t$ and $b = 1/t$ are both transcendental with $a^b = 2$ algebraic.

  Also a^b may be transcendental: fix a transcendental number a; the set of $c \in \mathbb{R}$ with a^c algebraic is countable, hence the set of $b \in \mathbb{R}$ with a^b transcendental is not countable, therefore it contains transcendental elements.
  Remark. A theorem of transcendental number theory (Gel'fond – Schneider, 1934) states that if a and b are algebraic with $a \neq 0$, $b \notin \mathbb{Q}$, and $\log a \neq 0$, then $a^b = e^{b\log a}$ is transcendental. For instance $2^{\sqrt{2}}$ is transcendental, also $e^{\pi} = (-1)^{-i}$ is transcendental.

- Problem 4.10 p. 48.

  If $K(\alpha, \beta)$ is a simple extension of K, it can be written $K(\gamma)$ for some $\gamma \in K(\alpha, \beta)$. Since $K(\alpha, \beta)$ is not an algebraic extension of K (it contains the transcendental element β), it follows that γ is transcendental over K.

  Write $\alpha = P(\gamma)/Q(\gamma)$. Since γ is root of the polynomial $P(x) - \alpha Q(x)$, it is algebraic over $K(\alpha)$ and the extension $K(\gamma) : K(\alpha)$ is algebraic. From Theorem 4.7 we deduce that $K(\alpha) : K$ is not an algebraic extension, hence α is transcendental over K.

  This means that the only elements in a simple transcendental extension $K(\gamma) : K$ which are algebraic over K are the elements in K. See also exercises 4.8 and 5.5.

- Problem 4.11 p. 48.

  Take $L = K(x)$ (the field of rational fractions in one variable over K) and τ the monomorphism which maps x to x^2:
  $$\tau\left(\frac{P(x)}{Q(x)}\right) = \frac{P(x^2)}{Q(x^2)}.$$
  The image of τ is the subfield $K(x^2)$, and L is a quadratic extension of $K(x^2)$.