# Number Theory 2

22.7.2024

WRITTEN EXAM, 1ST TRY

SKETCH OF SOLUTIONS*

(These are not necessarily full solutions and they do not serve as a grading scheme for the exam. There may be better/nicer/cooler solutions as well.)

Problem 1 a) Let $L/K$ be a finite field extension.

This means: $[L:K] = \dim_K L = n \in \mathbb{N}_{>0}$.

We need to show that $\forall \alpha \in L, \exists f \in K[x]\setminus\{0\}$ with $f(\alpha)=0$.

Let $\alpha \in L$ be arbitrary, (non zero). Consider the elements:

$$1, \alpha, \dots, \alpha^n \in L.$$

- If they are distinct, then, as they are $n+1$ vectors in the $n$-dimensional $K$-vector space $L$, they are linearly dependent. Thus there exist $c_0, \dots, c_n \in K$, not all zero, s.t. $f(\alpha)=0$ with $f = \sum_{i=0}^{n} c_i x^i \in K[x]\setminus 0$.

- If they are not distinct, then the order of $\alpha$ in $L^\times$ is finite, say $d$. It follows $f(\alpha)=0$, for $f = x^d - 1 \in K[x]\setminus 0$.

An example of an infinite algebraic extension is the algebraic field of algebraic numbers:

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$$

over $\mathbb{Q}$. This is algebraic, but infinite, as it contains $\mathbb{Q} \subset \mathbb{Q}(\zeta_p) \subset \overline{\mathbb{Q}}$, with $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$ for every prime $p$.

1b. First, write $L := \mathbb{Q}(\sqrt{5}, \sqrt{7})$ and note that:

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt{5})]\cdot[\mathbb{Q}(\sqrt{5}):\mathbb{Q}] = 2\cdot 2 = 4.$$

Claim: the primitive element is $\sqrt{5}+\sqrt{7} =: \alpha$

We have $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset L$. 3 strategies to show $\mathbb{Q}(\alpha) = L$:
So $[\mathbb{Q}(\alpha):\mathbb{Q}] \in \{2, 4\}$.

(A) Show $\mathbb{Q}(\sqrt{5},\sqrt{7}) \subset \mathbb{Q}(\alpha)$. (B) Show $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$

(C) Show that $\mathbb{Q}(\alpha)$ is fixed only by the trivial el. of $\mathrm{Gal}(L/\mathbb{Q})$

(A) Solve the linear systems $\sqrt{5} = \sum_{i=0}^{3} x_i \cdot \alpha^i$ , $\sqrt{7} = \sum_{i=0}^{3} y_i \cdot \alpha^i$ over $\mathbb{Q}$.

$\alpha^0 = 1$, $\alpha^1 = \sqrt{5}+\sqrt{7}$, $\alpha^2 = 12 + 2\cdot\sqrt{35}$, $\alpha^3 = 5\sqrt{5} + 3\cdot 5\sqrt{7} + 3\cdot 7\cdot\sqrt{5} + 7\sqrt{7} = 26\cdot\sqrt{5} + 22\sqrt{7}$.

$\Rightarrow \sqrt{5} = \dfrac{\alpha^3 - 22\cdot\alpha}{4}$ and $\sqrt{7} = \dfrac{\alpha^3 - 26\alpha}{-4}$.

(B) Because $\sqrt{5}, \sqrt{7}, \sqrt{35}$ are linearly independent over $\mathbb{Q}$ $\Rightarrow$

$\Rightarrow 1, \alpha, \alpha^2$ are algebraically independent over $\mathbb{Q} \Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] \neq 2$.

(C) $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ maps $\sqrt{5}$ to $\pm\sqrt{5}$ and $\sqrt{7}$ to $\pm\sqrt{7}$.

So $\sigma(\sqrt{5}+\sqrt{7}) = \sqrt{5}+\sqrt{7} \Rightarrow \sigma = id \Rightarrow \mathbb{Q}(\alpha) = L$

1c. We know that every finite extension of a finite field $\mathbb{F}_q$ is of the form $\mathbb{F}_{q^n}$. We also know that $\mathbb{F}_q$ consists of all the roots of the polynomial $x^q - x$.

Because $(x^{10}-1)' = x^9 \neq 0$, $x^{10}-1$ has 10 distinct roots, so it cannot split over $\mathbb{F}_9$.

The next smallest extension of $\mathbb{F}_9$ is $\mathbb{F}_{81}$, which is the splitting field of $x^{81} - x$, so also of $x^{80} - 1$.

We have $x^{80} - 1 = (x^{10})^8 - 1^8 = (x^{10}-1)(x^{70} + x^{60} + \dots + 1)$

So $x^{10}-1$ splits into linear factors in $\mathbb{F}_{81}$, which is thus its splitting field.

$\boxed{\text{Problem 2}}$ a. Degree two extensions are always normal, because if a polynomial $f$ of degree 2 has one root $\alpha \in L$, then $f = (x-\alpha)\cdot(x-\beta)$ in $L[x]$.

So, if $L/K$ with $[L:K]=2$ is not Galois, then $L/K$ is not separable. In part, $\operatorname{char} K > 0$ and $\# K = \infty$ (finite fields are perfect)

Take: $K = \mathbb{F}_2(t)$ the field of rational functions over $\mathbb{F}_2$ in the variable $t$. Take then the irreducible polynomial $f = x^2 - t \in K[x]$, and let $L = K[x]/(f)$.

by Eisenstein for the prime el. $t$

Then $f$ is purely inseparable, because $f' = 0$, so $L/K$ is not separable, thus not Galois.

2b. No, there are not: Let $K$ be a field with $\operatorname{char} K = 3$

Assume $\operatorname{ord}_{K^\times}(\zeta) = 12$.

Then $\zeta^{12} = 1$ and $\zeta^i \neq 1$ for $0 < i < 12$.

But $\zeta^{12} - 1 = (\zeta^4 - 1)^3 = 0$, thus $\zeta^4 = 1$ $\lightning$.

2c. We may use $\deg(\Phi_{12}) = \varphi(12) = \#(\mathbb{Z}/12\mathbb{Z})^\times = 4$.

We have: $x^{12} - 1 = (x^6-1)(x^6+1) = (x^3-1)(x^3+1)(x^6+1) =$

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

From $x^{12} - 1 = \prod_{d \mid 12} \Phi_d$ we get $\Phi_{12} = x^4 - x^2 + 1$

Alternative: $\Phi_{12} = \prod_{(k,12)=1} (x - \zeta_{12}^k)$. So $k \in \{1, 5, 7, 11\}$.

using $\zeta_{12} = -\zeta_{12}^7$, $\zeta_{12}^5 = -\zeta_{12}^{11}$, $\zeta_{12}^6 = -1$, etc. one gets

$$\Phi_{12} = x^4 - x^2 + 1$$

2d. Write $\zeta := \zeta_{12}$

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/12\mathbb{Z})^{\times} \simeq (\mathbb{Z}/3\mathbb{Z})^{\times} \times (\mathbb{Z}/4\mathbb{Z})^{\times} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

$$\mathrm{mPol}(\zeta_{12}) = \Phi_{12} = x^4 - x^2 + 1$$

Its roots are $\zeta, \zeta^5, \zeta^7, \zeta^{11}$, and each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is determined by the image of $\zeta$. Set $\sigma_i : \mathbb{Q}(\zeta) \longrightarrow \mathbb{Q}(\zeta)$.

$$\zeta \longmapsto \zeta^i$$

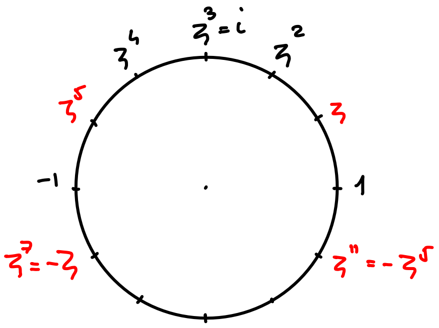
$$G := \mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) = \{ id = \sigma_1, \sigma_5, \sigma_7, \sigma_{11} \} \text{ and } \sigma_i^2 = id \ \forall i.$$

This means there are, besides $G$ and $\{id\}$, 3 subgroups:

$$\langle \sigma_5 \rangle, \ \langle \sigma_7 \rangle, \ \langle \sigma_{11} \rangle$$

For each $\sigma_i$ we have $\sigma_i(\zeta) = \zeta^i$ and $\sigma_i(\zeta^i) = \zeta$.

in particular $\sigma_i(\zeta + \zeta^i) = \zeta^i + \zeta$, thus.




We "see" that $\zeta + \zeta^5 = i \notin \mathbb{Q}$, so

$$\mathbb{Q}^{\langle \sigma_5 \rangle} = \mathbb{Q}(i)$$

Similarly: $\zeta + \zeta^{11} = \sqrt{3} \notin \mathbb{Q}$, so

$$\mathbb{Q}^{\langle \sigma_{11} \rangle} = \mathbb{Q}(\sqrt{3})$$

For $\sigma_7$ we can look systematically, by using the fact, that $1, \zeta, \zeta^2, \zeta^3$ is a basis of $\mathbb{Q}(\zeta)/\mathbb{Q}$.

So
$$\begin{aligned}\sigma_7(a + b\zeta + c\zeta^2 + d\zeta^3) &= a + b\zeta^7 + c\cdot\zeta^{14} + d\cdot\zeta^{21} = \\ &= a + b(-\zeta) + c\cdot\zeta^2 + d(-\zeta^3) \\ &= a - b\zeta + c\cdot\zeta^2 - d\zeta^3.\end{aligned}$$

So $\sigma_7(\alpha) = \alpha \iff \alpha = a + c \cdot \zeta^2$

In particular, for $a=0, c=1$, we get $\mathbb{Q}(\zeta^2) = \mathbb{Q}^{\langle \sigma_7 \rangle}$

So the fields $E$ with $\mathbb{Q} \subset E \subset \mathbb{Q}(\zeta)$ are

$$\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\zeta^2), \mathbb{Q}(\zeta).$$

Because $\mathbb{Q}$ is a prime field, there are no further subfields.

$\boxed{\text{Problem 3}}$ a. We have that $K = \mathbb{Q}(i)$ contains $i$, a primitive 4th root of unity. Char $K = 0$, so no worries.
We have $L = K(\sqrt[4]{2})$, with $\sqrt[4]{2}$ a root of $x^4 - 2 \in K[x]$.
Thus $L/K$ is cyclic of degree $d$, with $d \mid 4$. (Prop 4.8/3)
It remains to see if $d = 1, 2$ or $4$.
But $x^4 - 2$ is irreducible* over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.
Also $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ and $\mathbb{Q}(i) \not\subseteq \mathbb{R}$, so

$$\underbrace{\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt[4]{2})}_{4} \underbrace{\subsetneq \mathbb{Q}(i, \sqrt[4]{2})}_{2} \text{ has degree } 8.$$

* by Eisenstein for $p = 2$

Note: $2 = (1+i)(1-i)$ is not prime in $\mathbb{Q}(i)$.

$$\underbrace{\underbrace{\mathbb{Q} \subset K}_{2} \subset L}_{8} \quad \text{implies } [L:K] = 4, \text{ so } \mathrm{Gal}(L/K) \cong \mathbb{Z}/4\mathbb{Z}.$$

3b. A basis is given by the powers of a root of $x^4 - 2$, which has $x^4 - 2$ as minimal polynomial.

For instance: $1, \sqrt[4]{2}, \sqrt[4]{4} = \sqrt{2}, \sqrt[4]{8} = \sqrt{2} \cdot \sqrt[4]{2}$

$\boxed{\text{Call } r := \sqrt[4]{2}.}$

3c. We have that each $\mathbb{Q}(i)$-automorphism $\sigma$ of $L$ is determined by $\sigma(r) \in \{r, i r, -r, -ir\}$
We have: $\mathrm{id}(r) = r$, $\sigma_1(r) = ir$, $\sigma_2(r) = -r$, $\sigma_3(r) = -ir$.
To compute the trace we use, because $L/K$ is separable,

$$tr_{L/K}(i + r) = \sum_{\sigma \in G} \sigma(i + r), \quad G = \mathrm{Gal}(L/K)$$

So $tr_{L/K}(i + r) = (i + r) + (i + ir) + (i - r) + (i - ir) = 4i$.

Alternatively, we compute the matrix of $\cdot(i+r) : L \longrightarrow L$ with respect to the basis $1, r, r^2, r^3$, which is

$$M = \begin{pmatrix} i & 0 & 0 & 2 \\ 1 & i & 0 & 0 \\ 0 & 1 & i & 0 \\ 0 & 0 & 1 & i \end{pmatrix}$$ , whose trace is $4i$.

(Notice that the norm is $1-2=-1$)

3d. We use Hilbert 90, because we have a cyclic Galois extension:

$$N_{L/k}(b) = 1 \iff \exists a \in L^\times : b = \frac{a}{\sigma(a)}$$

where $\sigma$ is a generator for $Gal(L/k)$.

In our case, choose $\sigma := \sigma_1$ with $\sigma_1(r) = ir$.

We then choose $a = 1 + r^2$ and obtain,

$$\sigma(a) = \sigma(1+r^2) = \sigma(1) + \sigma(r^2) = 1 + (\sigma(r))^2 = 1 - r^2.$$

So $$b = \frac{1+r^2}{1-r^2}$$

As $r^2 = \sqrt{2}$, we get:

$$b = \frac{1+\sqrt{2}}{1-\sqrt{2}} = \frac{(1+\sqrt{2})^2}{1-2} = -(1+2\sqrt{2}+2) = -3-2\sqrt{2}.$$

(To double check: we may also take $-b = 3+2\sqrt{2}$, use $(r^2)^2 = 2$:

$$M(-b) = \begin{pmatrix} 3 & 0 & 4 & 0 \\ 0 & 3 & 0 & 4 \\ 2 & 0 & 3 & 0 \\ 0 & 2 & 0 & 3 \end{pmatrix}$$

so $$\det M(-b) = 3 \cdot \det \begin{pmatrix} 3 & 0 & 4 \\ 0 & 3 & 0 \\ 2 & 0 & 3 \end{pmatrix} + 2 \cdot \det \begin{pmatrix} 0 & 4 & 0 \\ 3 & 0 & 4 \\ 2 & 0 & 3 \end{pmatrix} =$$

$$= 3 \cdot 3 \cdot (3\cdot 3 - 2 \cdot 4) + 2(-4)\cdot(3 \cdot 3 - 2 \cdot 4) = 9 \cdot 1 - 8 \cdot 1 = 1 \;)$$

Alternatively, if one just remembers the definition, compute the norm of a generic element $a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt{2}\cdot\sqrt[4]{2}$ as the determinant of: $\begin{pmatrix} a & 2d & 2c & 2b \\ b & a & 2d & 2c \\ c & b & a & 2d \\ d & c & b & a \end{pmatrix}$. Put in some zeros and try to solve.