CVIKA III

I. POČÍTÁNÍ S ČÍS. TĚLESY

1. $\mathcal{O}_K$ & DISKRIMINANT

A) $K = \mathbb{Q}(\sqrt{d})$, d BEZČTV. PAK $\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \ (4) \\ \mathbb{Z}\left[\frac{+1+\sqrt{d}}{2}\right] & d \equiv 1 \ (4) \end{cases}$

SPOČTI $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})$.

B) UVAŽUJME $f(x) = x^3 - x - 1$, ZNAČME α KOŘEN f.
SPOČTI $\mathrm{disc}(1, \alpha, \alpha^2)$ A URČI $\mathcal{O}_{\mathbb{Q}(\alpha)}$.

C) TOTÉŽ PRO $x^5 - x - 1$.

D)* SPOČTI DISKRIMINANT $f(x) = x^n + ax + b$, $a, b \in K$
– ZA PŘEDP. IRED. & SEPAR.

$$\mathrm{disc}(f(x)) = (-1)^{\binom{n}{2}} \left(n^n b^{n-1} + (-1)^{n-1} (n-1)^{n-1} a^n \right)$$

E)* K ČÍS. TĚL.
ZNAMÉNKO $\mathrm{disc}(K/\mathbb{Q})$ JE $(-1)^s$, KDE $2s$ JE POČET KOMPL. NEREÁLNÝCH VNOŘENÍ $K \hookrightarrow \mathbb{C}$.

F)* (STICKELBERGEROVA VĚTA)
$\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) \equiv 0, 1 \pmod 4$.
(JDE POUŽÍT V A))

2. PRVOIDEÁLY.

A) POPIŠ, JAK SE ROZKLÁDAJÍ PRVOIDEÁLY V $\mathbb{Q}(\sqrt{m})$, m BEZČTV.

B) TOTÉŽ V $\mathbb{Q}(\alpha)$, $\alpha^3 + 10\alpha + 1 = 0$.

C) $x^2 + y^2 = p$ MÁ ŘEŠENÍ V $\mathbb{Z}$ $\iff$ $p \equiv 1 \pmod 4$
$x^2 + 2y^2 = p$ — " — $\iff$ $p \equiv 1, 3 \pmod 8$

CVIKO TTT 2.

3.) TŘÍDOVÁ GRUPA, ATD.

A) POUŽIJ MINKOWSKÉHO NEROVNOST K DŮ., ŽE $\mathbb{Z}[i]$ JE OIHI.

B) POPIŠ $Cl(\mathbb{Z}[\sqrt{-5}])$

C)* A CO KUBICKÁ ROZŠÍŘENÍ?
PRO JAKÉ HODNOTY DISKRIMINANTU URČITĚ DOSTANEME OIHI?

D)* VYŘEŠ V $\mathbb{Z}$ ROVNICI $x^2+5=y^3$.

E) $\mathbb{Q}(\sqrt{-23})$ MÁ TŘÍDOVÉ ČÍSLO 3.

F) K ČÍS. TĚL. DŮ, ŽE $\exists$ KON. ROZŠ. L/K T.Ž. VŠECHNY IDEÁLY O_K JSOU HLAVNÍ V O_L.

G)* $K=\mathbb{Q}(\sqrt{-1},\sqrt{5})$. DŮ.:
- $O_K=\mathbb{Z}[\sqrt{-1},\frac{1+\sqrt{5}}{2}]$.
- JEDINÁ PRVOČÍSLA (ZE $\mathbb{Z}$), KT. SE V K VĚTVÍ, JSOU 2 A 5, JEJICH INDEXY VĚTVENÍ $=2$.
- K JE NEROZVĚTVENÉ NAD $\mathbb{Q}(\sqrt{-5})$.

4.) VĚTA O JEDNOTKÁCH.

A) DŮ, ŽE $\#\mu(K)<\infty$ (PŘÍMO, BEZ POUŽITÍ VĚTY)

B) a JE JEDNOTKA $\Leftrightarrow N_{K/\mathbb{Q}}\,a=\pm 1$.

C) $K=\mathbb{Q}(\sqrt{d})$, d BEZČTV. POPIŠ $O_K^{\times}$.

CVIKO III 3.

5.) VALUACE.

A) K ÚPLNÉ TĚLESO S NEARCH. VALUACÍ $|\cdot|$.
PAK $\sum a_n$ KONVERGUJE $\iff$ $a_n \longrightarrow 0$.

B) KOLIK JE $1+2+2^2+\dots$ V $\mathbb{Q}_2$?

C) DK., ŽE -1 JE ČTVEREC V $\mathbb{Q}_5$.

D) V $\mathbb{Q}_p$ DEFINUJME $\exp(x) = 1+x+\frac{x^2}{2!}+\dots+\frac{x^n}{n!}+\dots$

TATO SUMA KONVERGUJE PRO $|x| < p^{-\frac{1}{p-1}}$ (DOKAŽ!)

E) DK. SOUČTOVOU FORMULI PRO ČÍS. TĚLESO
(ZE SOUČ. FORM. PRO $\mathbb{Q}$ A TVRZENÍ O ROZŠIŘOVÁNÍ VALUACÍ)

F)* DK. OSTROWSKÉHO VĚTU.

G) KOLIK JE $1+2\cdot 3+3^2+\dots+3^{2n}+2\cdot 3^{2n+1}+\dots$ V $\mathbb{Q}_3$?

H) UVAŽUJME $\mathbb{Q}_p$. POKUD MÁME PERIODICKOU ŘADU
$\sum a_i p^i$, KDE $a_i \in \{0,1,\dots,p-1\}$, (TEDY $a_{i+m}=a_i$
PRO NĚJ. m A VŠECHNA i), PAK $\sum a_i p^i \in \mathbb{Q}$.

I) DK., ŽE $\# \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} = 4$ .. POKUD $p \neq 2$

8 .. POKUD $p = 2$.

CVIKO TTT 4

6. ZÚPLNĚNÍ + LOKÁLNÍ TĚLESA.

A) POPIŠ VŠECHNA n T.Ž. $\mathbb{Z}_7$ OBSAHUJE n-TÉ ODMOCNINY Z 1.

B)* DOK., ŽE POKUD JE K TĚLESO, ÚPLNÉ VZHLEDEM K ARCH. VALUACI, PAK $K \simeq \mathbb{R}$ NEBO $\mathbb{C}$ A VALUACE ~~ROZŠÍŘENÍ~~ JE EKVIV. „NORMÁLNÍ" ABS. HODNOTĚ.

C) DOK., ŽE POKUD JE K LOKÁLNÍ TĚLESO $\mathrm{char}=0$ VZHL. K NEARCH. VALUACI, PAK $K \simeq$ KON. ROZŠ. $\mathbb{Q}_7$ A VALUACE NA K JE EKVIV. JEDNOZN. ROZŠÍŘENÍ $|\cdot|_7$.

D) K LOKÁLNÍ TĚLESO. DOK., ŽE PAK JE SFÉRA $S = \{x \in K \mid |x| = 1\}$ KOMPAKTNÍ V K.

E) DOK., ŽE $\mathbb{Q}_7^{al}$ NENÍ ÚPLNÉ.
(HINT: $\zeta_n =$ PRIMITIVNÍ n-TÁ ODM. Z 1.
$K/\mathbb{Q}_7$ KON. $\Rightarrow \zeta_n \in K$ JEN PRO KON. MN. n.
$\sum \zeta_n 7^n$ JE CAUCHYOVSKÁ, ALE $\sum \notin \mathbb{Q}_7^{al}$.)

F) PRO KTERÁ $a \in \mathbb{Z}$ MÁ ROVNICE $7x^2 = a$ ŘEŠENÍ V $\mathbb{Z}_7$? A PRO KTERÁ $a \in \mathbb{Q}$ MÁ ŘEŠENÍ V $\mathbb{Q}_7$?

G) DOK., ŽE $\forall$ LOKÁLNÍ TĚLESO JE ÚPLNÉ.

H) BUĎ $L = \mathbb{Q}(\vartheta)$, $\vartheta^4 = 14$. DOKAŽ:
- $11 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, $L_{\mathfrak{p}_1} = L_{\mathfrak{p}_2} = \mathbb{Q}_{11}$, $[L_{\mathfrak{p}_3} : \mathbb{Q}_{11}] = 2$
- $13 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$
- $5 = \mathfrak{p}_1\mathfrak{p}_2$, $[L_{\mathfrak{p}_i} : \mathbb{Q}_5] = 2$, $i = 1, 2$