

Семинар 0 (05.02.2026)

- 1) Проверьте, что 5987 — простое и кэлидовое $\left(\frac{3766}{5987}\right)$
- 2) Докажите, что $x^2 + 3 \equiv 0(p)$ имеет решение $\Leftrightarrow p \equiv 1(3)$.
- 3) Пусть p и $a \in \mathbb{Z}$. Докажите, что число решений $\sum$ сравнения $ax^2 + bx + c \equiv 0(p)$ равно $1 + \left(\frac{b^2 - 4ac}{p}\right)$
- 4) Упр 3, 4, 5 из ANTO
- 5)* Упр 2 из ANTO.

- Семинср 1 (12.02.2026) 1) Док-т через 1.2.1 из АНТ 1 (гип. 5)
- 2) $R[x] = \left\{ \sum_{i \geq 0} a_i x^i \mid a_i \in R \right\}$ - кольцо форм. степеней не упрощ., что то есть кон. число $a_i \neq 0$!
- Δ -тв, что R локально $\Rightarrow R[x]$ локально.
- Указ: $f \in R[x]$ обратим, если $f(0) = a_0$ обратим.
- ($\Leftarrow$ тоже верно).
- 3) Δ -тв, что кольцо $\mathbb{Z}[\sqrt{-2}]$ факториально, а кольцо $\mathbb{Z}[\sqrt{p}]$, где $p \equiv 1(4)$ простое - нет.
- 4) Δ -тв, что в кольце $\mathbb{Z}[x]$ простые делятся на-т $f(x) = (x-c_1) \cdot \dots \cdot (x-c_n) \pm 1$, где c_i разл. целые числа.
- 5)* Δ -тв, что в $\mathbb{Z}[x]$ на-т $g(x) = (x-c_1) \cdot \dots \cdot (x-c_n) \pm 1$, где $c_1, \dots, c_n$ - разл. целые, простое при $n \neq 2$ и 4 .
Наиб. разл. простое не простое при $n = 2$ и 4 .

Землеп 2 (19.02.2026)

- 1) R -вн. гласан кон $|R| < \infty \Rightarrow R$ -вн.
- 2) $\mathbb{F}$ -вн, $\forall i \in I$ R_i - гласанн. конго $\mathbb{F}$.
Тогд $R = \bigcap_{i \in I} R_i$ тнм гласанн.
- 3) Бил $d \in \mathbb{Z}$ сродо гн обспетр. Тогд $\mathbb{Z}[\sqrt{d}]$ нг гн-сн гласанн. $\forall d \equiv 1(4)$.
- 4) $\mathbb{F}$ -вн, $a = \text{const} \in \mathbb{F}^n$. Тогд конго
 $\mathcal{Q} = \left\{ \frac{f}{g} \mid f, g \in \mathbb{F}[x_1, \dots, x_n], g(a) \neq 0 \right\}$ нгсдн.

Семинер 3 (26.02.2026)

1) Упр 2 из лекции АНТ 3

2) Пусть $E = \mathbb{Q}[\sqrt{2}, \sqrt{5}]$, $\beta = \sqrt{2} + \sqrt{5}$. Найти $\chi_{E/\mathbb{Q}}^{\beta}(t)$ и $\chi_{E/\mathbb{Q}[\sqrt{5}]}^{\beta}(t)$.

3)* $\varepsilon = e^{2\pi i/3}$. Найти все собственные значения в $\mathbb{Z}[\varepsilon]$.
(разберитесь со следствием Занятия 1)

Семинар 4 (04.03.2026) :

1) Для $m, n \in \mathbb{Z}$ свод. от кв-ров. Тогда

$$\mathbb{Q}[\sqrt{m}] \simeq \mathbb{Q}[\sqrt{n}] \Leftrightarrow m=n.$$

2) Найти $\text{disc}(\mathbb{Q}[\varepsilon]/\mathbb{Q})$, где ε — прим.
корень $x^3 = 1$.

3) При каких значениях λ

а) мн-н $t^3 - \lambda t + 2$ и $t^2 + \lambda t + 2$ имеют
общий корень?

б) мн-н $t^3 - 3t + \lambda$ имеет краткий корень?

4) Вычислить дискриминант мн-нов

а) $t^n + a$ б) $t^{n-1} + t^{n-2} + \dots + t + 1$

5*) Прочитать §2.4 и 2.5 в гл. 6 [Кос1]

и решить упр 3 из АНТ4, где сок → п т. 1.6.2
о вычислении дисперсии χ^2 .

Семинар 5 (12.03.2026) 0) Доредатил задаток из K/p

- 1) Доредатил задаток 5 (случај $|O_L: M| = 3$)
- 2) Најмалыи базис в O_L , есак $L = \mathbb{Q}[\theta]$,
гдѣ θ - корен m -~~к~~ x :

а) $t^3 + 3t^2 + 4t - 1$

б) $t^3 - t + 4$

в) $* t^3 + 3t - 2$

- 3) Брзат ли селекционировани кода

а) $\mathbb{Z}$ б) $\mathbb{Q}$ в) $\mathbb{Z}[\sqrt{5}]$ г) $\mathbb{Z}[\sqrt{5}]$

г) $\overline{\mathbb{Z}} \subset \mathbb{C}$ - цело заткение $\mathbb{Z}$ в $\mathbb{C}$

д) $F[x], F[x_1, x_2], F[x^2, x^3]$, гдѣ F - поле?

4**) 1-го теорема Штейнсабегтега: $\text{disc}(\mathcal{O}_L/\mathbb{Z}) \equiv 0, 1 \pmod{4}$

Указание: а) пусть $x_1, \dots, x_n$ - каноническая база $\mathcal{O}_L$,

$\sigma_1, \dots, \sigma_n$ - $\mathbb{Q}$ -вложения L в $\mathbb{C}$, где $n = [L:\mathbb{Q}]$

Значит $\text{disc}(\mathcal{O}_L/\mathbb{Z}) = \det(T(x_i, x_j))$

$= (\det(\sigma_i(x_j)))^2 = (P - N)^2$, где P и N - числа
 в $\det(\sigma_i(x_j))$ со знаками "+" и "-" соответственно.

б) $E \supset L$ и $\varphi \in \text{Gal}(E/\mathbb{Q}) \Rightarrow \varphi(P+N) = P+N, \varphi(PN) = PN \Rightarrow \frac{P+N}{PN} \in \mathbb{Q}$.
 ← по п. 3а).

в) $\exists \tau \in \text{Gal}(E/\mathbb{Q})$, что $P+N, PN \in \mathbb{Q} \Rightarrow P+N, PN \in \mathbb{Z}$.

г) В $(P+N)^2$ члены $P+N$ и PN и возможно
 что PN - число, но возможно и $\frac{1}{2}$.

Семинар 6 (19.03.2026)

- 1) Пусть A -св. $K = \mathbb{Q}(A)$, L — кон. сеп. расщ. K ,
 $B = \overline{A}^L$, $I_1, I_2 \trianglelefteq A$. Тогда $I_1 B = I_2 B \Leftrightarrow I_1 = I_2$.
- 2) $I \trianglelefteq A$, $J, K \trianglelefteq A$. Тогда, что $IJ \subseteq P \Rightarrow$
 $I \subseteq P$ или $J \subseteq P$.
- 3) Пусть I, J, K — идеалы факториальной кольца A . Тогда,
 $I \cap (J + K) = (I \cap J) + (I \cap K)$ и $I + (J \cap K) = (I + J) \cap (I + K)$.
- 4) Пусть $0 \neq I \trianglelefteq A$ — факториально. Тогда, что
в A/I любой идеал идеал.
- 5)* Тогда, что в $A_{\mathbb{Z}} = \overline{A}^{\mathbb{Z}}$ любой идеал идеал.

6) а) (Кукер 65) Если $P \nsubseteq O_L$, где L -числовое анр. число,
то $P \cap \mathbb{Z} \neq \emptyset$

б) При заданной галекангово кольцо B такое, что
 $B \cong \mathbb{Z}$, $P \subseteq B$, то $P \cap \mathbb{Z} = \emptyset$.

7) ^{***} (Грюк Софи-Мермен) Пусть p и $q = 2p+1$ -простые
числа. Если $x^p + y^p + z^p = 0 \Rightarrow p \mid xyz$.

Указ: а) Если $x \not\equiv 0 (q) \Rightarrow x^p \equiv \pm 1 (q)$

б) $x^p + y^p + z^p = 0 \Rightarrow q \mid xyz$ "А"
Уск-но hab. la bugs - $x^p = y^p + z^p = (y+z)(y^{p-1} - y^{p-2}z + \dots - yz^{p-2} + z^{p-1})$

в) $(A, A) = 1$, where $\exists r \mid (A, A) \Rightarrow y = -z/r \Rightarrow py^{p-1} \equiv 0 (r) \dots$ ∇

г) $(A, A) = 1 \Rightarrow A = a^p$ и $A = d^p$ и $x = -ad$ (аналогично

$y = -b^p, z = -c^p$.

д) $q \mid abc$ (гол. до). Прими и умножившись с $q \mid xyz$.

Семинар 7 (26.03.2026): 1) Упр 1 из ANT 8.

2) Разложить $\mathbb{Q}_L$ на простые идеалы в $\mathbb{Q}_L$,
где а) $L = \mathbb{Q}[\sqrt{11}]$ б) $L = \mathbb{Q}[\sqrt{13}]$.

3) $L = \mathbb{Q}(\sqrt{m})$, m — целое свод. от идеалов $\neq 1$.
Разложить (в зав от m) на простые в $\mathbb{Q}_L$
идеал $I = 2B$.

4) Пусть $AKBL$, где A — простое число, $|L:K| = n$.

Для $P \in A$: $PB = Q^n$, где Q — простой идеал в B .

(P в B не разветвлен в L). Δ — те, что $\forall$ подг E :
 $K \subseteq E \subseteq L$, то P в E не разветвлен и в E .

5*) Упр 2 и 3 из ANT 8.

Семинар 8
02.04.2026

1) Пусть $L = \mathbb{Q}[\sqrt{997}]$. Д-т, что $113 \mathcal{O}_L$ — идеал и делит $\mathcal{O}_L$.

2) Пусть p — простое число, $L = \mathbb{Q}[\sqrt{m}]$

Док-н, что $p \mathcal{O}_L = (\mathfrak{p}, \sqrt{m})^2 \Leftrightarrow p \mid m$

$p \mathcal{O}_L = \mathfrak{p}_1 \mathfrak{p}_2$, если m — квадрат mod p

$p \mathcal{O}_L = \mathfrak{p}$ — идеал $\Leftrightarrow m$ — не квадрат mod p .

3) Д-т, что идеал $\mathcal{O}_L$ факторизуется, где $L = \mathbb{Q}[\sqrt{m}]$

и а) $m = -3$ б) $m = -7$ в) $m = 13$.

4*) Упр 1 и Упр 2 из ANT 10.

Семинар 9 (09.07.2026)

- ① Пусть $L = (\mathbb{Z}/11)[\sqrt{7}]$. Тогда $h_L = 2$. Найти $\text{Cl}(\mathcal{O}_L)$.
- ② Заданы идеалы $\mathfrak{p}_1, \mathfrak{p}_2$ в поле $K = \mathbb{Q}(\sqrt{m})$:
 $m = -43, -67, -163 \Rightarrow h_L = 1$.
- ③ Найти $\text{Cl}(\mathcal{O}_L)$, где $L = \mathbb{Q}[\sqrt{-21}]$.
- ④ Вып 1 а) из АНТ 10
- ⑤ ⁺ Вып 1 б) и Вып 2 из АНТ 10.

Семинар 10 (30.04.2026):

1) Тип $L = (\mathbb{Q}[\sqrt{d}])$. Усл-я existence O_L^* , observe
полюсу y -е $a^2 - b^2 d = -1$ имеет бесконечно
решений (a, b) при $d = 2$ и не имеет при $d = 3$.

2) Завершите решение н.б) y из ANT 11.

3) y из ANT 11

4) Найти не homomorphism PL class
 y -е class a) $x^2 - 7y^2 = 1$ б) $x^2 - 10y^2 = 1$ в) $x^2 - 13y^2 = 1$.

5)* Для первопр. class $\sum m$ -a class , $m > 2$ и $L = (\mathbb{Q}[\frac{1}{2}])$,

$$\Delta = \text{то, что } \text{disc} \left(\frac{O_L}{\mathbb{Z}} \right) = \frac{(-1)^{\varphi(m)/2} \cdot m^{\varphi(m)}}{\prod_{p|m} p^{\varphi(m)/(p-1)}}.$$

Семinar 11 (07.05.2026): 1) Рассмотрим $\Phi_G(t)$

2) Докажем, что $\notin \chi h_L$, где L -кривая расщ. ст. $\mathbb{F}$.

3) Пусть $\{ \}$ - крит. корни и-ой ст. $\mathbb{F}$. При каких условиях на $\mathbb{F}$ и кривое расщ. $\mathbb{Q}[\{ \}]$: $\mathbb{Q}$ -функционала, (т.е. его крит. Тангл функционала)?

Указ: Вспомогат., что $\mathbb{Z}_n^* \simeq (\mathbb{Z}_{p_1^{u_1}})^* \times \dots \times (\mathbb{Z}_{p_s^{u_s}})^*$, где $n = p_1^{u_1} \times \dots \times p_s^{u_s}$.

4)* Докажем, что $\forall n \in \mathbb{N} \exists$ нек. число простых p таких, что $p \equiv 1(n)$.

Указ: От обратного. Пусть $p_1, \dots, p_s$ - все такие числа.

а) $\exists a \in \mathbb{Z} : \Phi(a; P) \neq \pm 1$, где $P = \prod_{i=1}^s p_i$.

Б) Для $t = anP$ берется простое $p \mid \Phi_n(t)$, тогда
 $n = \text{ord}_p t$, т.е. n - мин.: $t^n \equiv 1 (p)$.

В) Берется $\psi \in \mathbb{Z} \setminus \mathbb{B}$.
