Algebraic Number Theory

You are encouraged to collaborate on solving the problems given as homework. However, the solutions should be written on your own and in your own words. Please send me your homework to my email before the next week's class.

♠ 2012/02/15

1, Let α, β be algebraic numbers such that β is conjugate to α. Show that α and β have the same minimal polynomial.

2, Let α be an algebraic number and let $p(x)$ be its minimal polynomial. Show that $p(x)$ has no repeated roots.

3, Let $f(x) \in \mathbb{Z}[x]$ and $g(x) \in \mathbb{Q}[x]$ be monic polynomials. If $g(x)|f(x)$. Show that $g(x) \in \mathbb{Z}[x]$. i.e., the minimal polynomial of any algebraic integer has coefficients in $\mathbb{Z}$.

4, Determine the ring of integers $\mathfrak{o}_k$ of the quadratic field $k = \mathbb{Q}[\sqrt{d}]$, where d is square-free integer. And compute the discriminant d_k.

5, $d_{K/k}(a_1, \cdots, a_n) \neq 0 \Leftrightarrow a_1, \cdots, a_n$ are k-linear independence.

6, (a) Show that $f(x) = x^3 + x^2 - 2x + 8$ is irreducible in $\mathbb{Q}[x]$.

(b), Let θ be a root of $f(x)$ and $k = \mathbb{Q}(\theta)$. Compute $d_k(1, \theta, \theta^2)$.

(c), Show that $4/\theta \in \mathfrak{o}_k$.

♠ 2012/02/22

7, $d_k \equiv 0$ or $1 \mod 4$.

8, For any $\mathfrak{a}, \mathfrak{b} \in J_k$, the following assertions $\mathfrak{a} \subset \mathfrak{b}, \mathfrak{a}\mathfrak{b}^{-1} \subset \mathfrak{o}_k$ and $\mathfrak{o}_k \subset \mathfrak{a}^{-1}\mathfrak{b}$ are equivalent.

9 Compute the principal ideal (6) as the product of the prime ideals in the ring of integers $\mathfrak{o}_k$where $k = \mathbb{Q}(\sqrt{-5})$.

10, Show that every nonzero prime ideal in $\mathfrak{o}_k$ contains exactly one integer prime.

11, Let $\mathfrak{a}$ be an integral ideal of $\mathfrak{o}_k$. Then (1) $Norm(\mathfrak{a}) \in \mathfrak{a}$. (2) If $Norm(\mathfrak{a})$ is a prime number; then $\mathfrak{a}$ is a prime ideal. Conversely, true or false?

♠ 2012/02/29

12, Find a prime ideal factorization of $(2), (5)$ in $\mathbb{Z}[i]$.

13, Define $\gcd(\mathfrak{a}, \mathfrak{b})$ to be the greatest common divisor of $\mathfrak{a}$ $\mathfrak{b}$, if $\mathfrak{c}|\mathfrak{a}, \mathfrak{c}|\mathfrak{b}$; and if $\mathfrak{d}|\mathfrak{a}, \mathfrak{d}|\mathfrak{b}$, then $\mathfrak{d}|\mathfrak{c}$. Show that

$$\mathfrak{a} + \mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b}).$$

14, Let $\mathfrak{a} = (a) = a\mathfrak{o}_k$ be a principal ideal of $\mathfrak{o}_k$. Then $N(\mathfrak{a}) = |N(a)|$.

15, Let $a = 1 + i, b = 3 + 2i$, and $c = 3 + 4i$ as elements of $\mathbb{Z}[i]$.

(1) Prove that the ideals $\mathfrak{a} = (a), \mathfrak{b} = (b)$, and $\mathfrak{c} = (c)$ are coprime in pairs.

(2) Compute the number of the quotient ring $\mathbb{Z}[i]/(\mathfrak{abc})$.

(3) Find a single element in $\mathbb{Z}[i]$ that is congruent to 1 modulo $\mathfrak{a}$, 2 modulo $\mathfrak{b}$, and 3 modulo $\mathfrak{c}$.

♠ 2012/03/07

16, Compute the class group and the class number of the following quadratic fields:

$$\mathbb{Q}(\sqrt{3}), \quad \mathbb{Q}(\sqrt{5}), \quad \mathbb{Q}(\sqrt{-3}), \quad \mathbb{Q}(\sqrt{-5}).$$

17, Show that $\mathbb{Q}(\sqrt{-23})$ has class number 3.

18, Compute the group W_k of roots of unity for quadratic fields $k = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer.

19, Find a unit in $\mathbb{Q}(\sqrt[3]{6})$ and show that this field has class number $h = 1$.

20, Compute the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{3})$.

21, There exist only finitely many number fields with bounded discriminant.

♠ 2012/03/15

22, Statement and show that the ration prime p decomposes in quadratic fields $\mathbb{Q}(\sqrt{d})$.

23, Show that

$$[\mathfrak{O}_K/\mathfrak{p}\mathfrak{O}_K : \mathfrak{o}_k/\mathfrak{p}] = [K : k].$$

♠ 2012/03/22

24, Let K be a finite Galois extension of $\mathbb{Q}$with Galois group G. For each prime ideal $\mathfrak{P}$ of $\mathfrak{O}_K$, let $I_\mathfrak{P}$ be the inertia group. Show that the groups $I_\mathfrak{P}$ generate G.

25, (1), Find the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ where $K = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$.

(2), Find the decomposition fields, inertia fields, decomposition groups and inertia groups of $(2), (5)$ for $K = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$ over $\mathbb{Q}$.

26, Suppose that the extension $K/\mathbb{Q}$ is normal and has a Galois group which is simple but not cyclic. Show that there is no rational prime p such that (p) remains prime in K.

27, Let $\zeta^n = 1$ and assume that

$$\alpha = \frac{\sum_{i=1}^{m} \zeta^{n_i}}{m}$$

is an algebraic integer. Show that either $\alpha = \zeta^{n_i}$ for each i or $\alpha = 0$.

♠ 2012/03/29

1, The $\mathfrak{p}$-adic valuation is nonarchimedean.

2, Let $|\cdot|$ be any valuation over any field k and $|\cdot|_\infty$ be the usual absolute value over $\mathbb{R}$. Then, for any $\alpha, \beta \in k$,

$$||\alpha| - |\beta||_\infty \leq |\alpha - \beta|.$$

3, A field k of nonzero characteristic has only nonarchimedean valuations.

4, Let $|\cdot|$ be any valuation over any field k. Then $|\cdot|$ is nonarchimedean iff $|1 + \alpha| < 1$ for any $|\alpha| < 1$.

5, Let $\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1} = \bar{\sigma}_{r_1+r_2+1}, \ldots, \sigma_{r_1+r_2} = \bar{\sigma}_n$ be embeddings of k. Let $|\cdot|_1, \ldots, |\cdot|_{r_1+r_2}$ be archimedean valuations induce by $\sigma_1, \ldots, \sigma_{r_1+r_2}$. Then $|\cdot|_1, \ldots, |\cdot|_{r_1+r_2}$ are pairwise inequivalent.

6, Let $\mathfrak{p}$ and $\mathfrak{q}$ be two distinct prime ideals of a number field k. Then the $\mathfrak{p}$-adic valuations $|\cdot|_\mathfrak{p}$ and $|\cdot|_\mathfrak{q}$ are inequivalent.

♠ 2012/04/05

7, Find $\alpha \in \mathbb{Q}$, such that $v_2(\alpha - 1/3) \geq 2, v_3(\alpha - 1/2) \geq 3$, and $|\alpha - 1|_\infty < 1/2$.

8, If a sequence α_n converges a nonzero element α withe respect to any nonarchimedean valuation over a field k, then we have $|\alpha| = |\alpha_n|$ for sufficiently large n.

9,

$$\begin{array}{rccc} \mathrm{ord}_\mathfrak{p} : & k & \longrightarrow & \mathbb{Z} \\ & \alpha & \longmapsto & \mathrm{ord}_\mathfrak{p}(\alpha). \end{array}$$

Then it is surjective.

10, $\mathfrak{o}_\mathfrak{p}$ (respectively, $\mathfrak{p}_\mathfrak{p}$) is the closure of $\mathfrak{o}_k$(respectively, $\mathfrak{p}$) in $k_\mathfrak{p}$.

11,

$$\mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \cong \mathfrak{o}_k/\mathfrak{p}.$$

♠ 2012/04/12

12, A valuation $|\cdot|$ on a field k is *discrete* if there is a $\delta > 0$ such that for any $\alpha \in k$

$$1 - \delta < |\alpha| < 1 + \delta \Longrightarrow |\alpha| = 1.$$

A non-archimedean valuation $|\cdot|$ on any field k is discrete if and only if $\mathfrak{p} = \{\alpha \in k : |\alpha| < 1\}$ is a principal ideal.

13, Let the polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k_{\mathfrak{p}}[X]$ be irreducible. Then

$$\max\{|a_i|_{\mathfrak{p}} \,:\, 0 \le i \le n\} = \max\{|a_0|_{\mathfrak{p}}, |a_n|_{\mathfrak{p}}\}.$$

14,

$$\mathfrak{o}_k = \bigcap_{\text{all prime ideals } \mathfrak{p}} \mathfrak{o}_{\mathfrak{p}}.$$

15, Show that Fermat equation $x^n + y^n = 1$ has infinitely many solutions over $\mathbb{Z}_p$ for any integer $n \ge 1$.

16, Write power series of the number $2/3$ and $-2/3$ as 5-adic numbers.

17, Show that the equation $x^2 = 2$ has a solution in $\mathbb{Z}_7$.

♠ 2012/04/19

18, Show that the exponential series

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

converges for $\mathrm{ord}_p(x) > \frac{1}{p-1}$ in $\mathbb{Q}_p$ and diverges elsewhere.

19, Show that for any prime p, there are $p-1$ distinct $(p-1)$-th roots of unity in $\mathbb{Z}_p$.

20, Suppose that $f(x) \in \mathbb{Z}[X]$, then $f(x) = 0$ has a solution in $\mathbb{Z}_p$ iff for any $n \ge 1$, the equation $f(x) \equiv 0(\mod p^n)$ has solutions in $\mathbb{Z}$.

21, Let $|\cdot|_1, \ldots, |\cdot|_m$ be distinct places of k. If

$$|\alpha|_1^{r_1} \cdots |\alpha|_m^{r_m} = 1,$$

for all $\alpha \in k^\times$, where r_i are real constants, then $r_1 = \cdots = r_m = 0$.

♠ 2012/04/26

22, (1), Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in k_{\mathfrak{p}}[X]$ be irreducible. If $a_n \in \mathfrak{o}_{\mathfrak{p}}$, then all $a_i \in \mathfrak{o}_{\mathfrak{p}}$.

(2), Let $\bar{f}(x) \in \mathbb{F}_{\mathfrak{p}}[X]$ be the polynomial obtained from $f(x)$ by reducing the coefficients of $f(x)$ modulo $\mathfrak{p}_{\mathfrak{p}}$. If $f(x) \in \mathfrak{o}_k[X]$ is monic and irreducible over $k_{\mathfrak{p}}$, then $\bar{f}(x)$ is a power of an irreducible polynomial in $\mathbb{F}_{\mathfrak{p}}[X]$.

23, Let $K_{\mathfrak{P}} \supset k_{\mathfrak{p}}$ be local fields. If $x \in K_{\mathfrak{P}}$, then $|x|_{\mathfrak{P}} = |N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}} x|_{\mathfrak{p}}^{1/[K_{\mathfrak{P}}:k_{\mathfrak{p}}]}$, and $\mathrm{ord}_{\mathfrak{p}}(N(x)) = f(\mathfrak{P}/\mathfrak{p})\mathrm{ord}_{\mathfrak{P}}(x)$.

24, Show that Theorem 2.35.

25, Show that (1), An Eisenstein polynomial $E(x)$ is irreducible and (2), Theorem 2.38.

♠ 2012/05/10

1, Let p_n be the nth positive prime in $\mathbb{Z}$, and let $\alpha^n = (\alpha_v^{(n)}) \in \mathbb{A}_{\mathbb{Q}}$ with $\alpha_v^{(n)} = p_n$ if $v = p_n$ and $\alpha_v^{(n)} = 1$ if $v \neq p_n$. The result is a sequence $\{\alpha^n\}$ of ideleds in $\mathbb{I}_{\mathbb{Q}}$. Show that this sequence converges to the idele $(1)_v$ in the topology of the adeles but not converges in the topology of the ideles.

2, Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be distinct places of a number field k and $x_1, \ldots, x_m \in k$. Let $\epsilon > 0$ be given. Then there exists $x \in k$ such that $|x - x_i|_{\mathfrak{p}_i} < \epsilon$ for $1 \leq i \leq m$ and $\mathrm{ord}_{\mathfrak{p}}(x) \geq 0$ for any $\mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$.

3, (Dedekind)

(1), Show that $f(x) = x^3 + x^2 - 2x + 8$ is irreducible in $\mathbb{Q}[x]$.

(2), Find the discriminant of $f(x)$.

(3), Let θ be a root of $f(x)$ and $k = \mathbb{Q}(\theta)$. Compute $d_{k/\mathbb{Q}}(\theta)$.

(4), Find the discriminant of $k = \mathbb{Q}(\theta)$.

(5), Show that $4/\theta, \frac{1}{2}(\theta^2 + \theta) \in \mathfrak{o}_k$.

(6), The prime 2 splits completely in k.

4, $\widehat{\mathbb{R}/\mathbb{Z}} \cong \mathbb{Z}$, i.e., every character of $\mathbb{R}/\mathbb{Z}$ is of form $x \mapsto e(mx)$ for some integer m.

4, $\widehat{\mathfrak{o}_v} \cong k_v^+/\mathfrak{D}_v^{-1}$.

5, Every additive quasicharacter χ_α of $\mathbb{R}^+$ is of form $\chi_\alpha : x \mapsto \chi_\alpha(x) = e(x\alpha)$ for some complex number α, i.e., the mapping

$$\mathbb{R}^+ \longrightarrow \widehat{\mathbb{R}^+} \quad \text{by} \quad \alpha \longmapsto \chi_\alpha$$

is an isomorphism of topological groups.

6, Every multiplicative character of the group $\mathbb{R}_+^\times$ (the multiplicative group of positive real numbers) is of form $x \mapsto x^s$ for some $s \in \mathbb{C}$.

(2) Every multiplicative character of the group $\mathbb{R}^\times$ (the multiplicative group of nonzero real numbers) is of form $x \mapsto \mathrm{sign}^\epsilon(x)|x|^s$ for some $s \in \mathbb{C}$ and $\epsilon = 0$, or 1.

7, (1) The circle group S^1 has no small subgroups, i.e., there is a neighborhood U of the identity $1 \in S^1$ such that the only subgroup of S^1 inside U is the trivial group $\{1\}$.

(2), Let G be a totally disconnected locally compact topological group. Prove that the kernel of any continuous homomorphism of $G \longrightarrow GL_m(\mathbb{C})$ contains an open subgroup.

8, If G is a compact topological abelian group, or if every element of G is of finite order, then every quasicharacter of G is a character.

2012/05/24

9, Let n be a positive integer and let

$$U(n) = \mathbb{R}_+^\times \prod_{p|n} U_p(n) \prod_{p\nmid n} \mathbb{Z}_p^\times$$

where $U_p(n) = \{x \in \mathbb{Z}_p^\times \,:\, x \equiv 1 \mod n\}$. And let

$$V(n) = \mathbb{R}_+^\times \prod_{p|n} U_p(n) \prod_{p\nmid n} \mathbb{Q}_p^\times.$$

Show that

$$\mathbb{I}_\mathbb{Q}/U(n)\mathbb{Q}^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

10, We will call $\chi : \mathbb{I}_k/k^\times \to S^1$ a character of finite order if there exists a positive integer m such that $\chi(x)^m = 1$ for all $x \in \mathbb{I}_k$. Then χ has finite order if and only if its restriction to $\mathbb{R}_+^\times$ is trivial.

11, (1) Let dx be an additive measure such that the measure $\mathbb{Z}_p$ is 1. Let $d^\times x$ be a multiplicative measure such that the measure $\mathbb{Z}_p^\times$ is 1. Then

$$d^\times x = \frac{p}{p-1}\frac{dx}{|x|_p}.$$

(2), Compute the integral

$$\int_{\mathbb{Z}_p} |x|_p^s \, dx.$$

12, Let $\chi_p(\alpha) = e(\lambda_p(\alpha))$ be an additive character of $\mathbb{Q}_p$ which defined in our note. Compute $k \in \mathbb{Z}$

$$\int_{\varpi^k U_p} \chi_p(x) \mathrm{d}x,$$

where ϖ is an uniformizer of $\mathbb{Z}_p$ and $U_p = \mathbb{Z}_p^\times$ is the unit group of $\mathbb{Z}_p$.

12, 12, 12, 12, 12, 12,
12,
12,
12, 12, 12,
12, 12,
12,
12, 12,