# MTH 617 Algebraic Number Theory

## Solutions of the exercises that appeared in the End Semester Examination

---

**1.** $\mathbb{Q}(\mathfrak{O}_K) = K$, $\mathbb{Q}(\mathbb{Z}) = \mathbb{Q}$, $K \neq \mathbb{Q}$ and $K$ is real, so that $\mathfrak{O}_K \subseteq \mathbb{R}$. It follows that $\mathbb{Z} \subsetneqq \mathfrak{O}_K$. Choose any $\beta \in \mathfrak{O}_K \setminus \mathbb{Z}$ and set $\xi := \beta - \lfloor \beta \rfloor$. We have $\xi \in \mathfrak{O}_K$ with $0 < \xi < 1$. But then given any real $\epsilon > 0$ we can choose a positive integer $n$ large enough so that $0 < \xi^n < \epsilon$.

**2.** Let $f(X) := X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0$, $a_i \in \mathbb{Z}$. Let $\gamma := a + b\alpha$, $a, b \in \mathbb{Z}$, $b \neq 0$. Since trace is additive, we have $\operatorname{Tr}(\gamma) = \operatorname{Tr}(a) + \operatorname{Tr}(b\alpha) = ad + b\operatorname{Tr}(\alpha)$. In order to compute the norm of $\gamma$ let me first note that $\gamma$ satisfies the non-zero monic polynomial

$$g(X) := b^d \left[ \left( \frac{X-a}{b} \right)^d + a_{d-1} \left( \frac{X-a}{b} \right)^{d-1} + \cdots + a_1 \left( \frac{X-a}{b} \right) + a_0 \right] \in \mathbb{Z}[X].$$

Since $f$ is irreducible (in $\mathbb{Z}[X]$), so is $g(X)$, i.e., $g(X) = \operatorname{minpoly}_{\gamma,\mathbb{Q}}(X)$. Therefore

$$\begin{aligned} \mathrm{N}(\gamma) &= (-1)^d \times \text{ the constant term of } g(X) \\ &= (-b)^d \left[ (-a/b)^d + a_{d-1}(-a/b)^{d-1} + \cdots + a_1(-a/b) + a_0 \right] \\ &= (-b)^d f(-a/b). \end{aligned}$$

**3.** For a number field $K$ of degree $d$ and signature $(r_1, r_2)$ and for a non-zero ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ there exists a non-zero element $\alpha$ in $\mathfrak{a}$, such that $|\mathrm{N}(\alpha)| \leqslant M_K \,\mathrm{N}(\mathfrak{a})$, where $M_K$ is the Minkowski constant given by $M_K = \dfrac{d!}{d^d} \left( \dfrac{4}{\pi} \right)^{r_2} \sqrt{|\Delta_K|}$. Since every non-zero element of $\mathfrak{O}_K$ has non-zero integral norm, taking $\mathfrak{a} = \mathfrak{O}_K$ gives us $1 \leqslant |\mathrm{N}(\alpha)| \leqslant \dfrac{d!}{d^d} \left( \dfrac{4}{\pi} \right)^{r_2} \sqrt{|\Delta_K|}$, i.e., $|\Delta_K| \geqslant \left[ \dfrac{d^d}{d!} \left( \dfrac{\pi}{4} \right)^{r_2} \right]^2$. Let us now specialize on cubic fields, i.e., to the case $d = 3$.

**Case 1:** Signature of $K$ is $(r_1, r_2) = (1, 1)$.

Sign of $\Delta_K$ is $(-1)^{r_2} = -1$. Therefore $\Delta_K \leqslant - \left[ \dfrac{3^3}{3!} \left( \dfrac{\pi}{4} \right) \right]^2 = -12.4912180701\ldots$, i.e., $\Delta_K < -12$.

**Case 2:** Signature of $K$ is $(r_1, r_2) = (3, 0)$.

Sign of $\Delta_K$ is $(-1)^{r_2} = 1$. Therefore $\Delta_K \geqslant \left( \dfrac{3^3}{3!} \right)^2 = 20.25$, i.e., $\Delta_K > 20$.

**4.** [if] It is sufficient to show that every non-zero prime ideal $\mathfrak{p}$ of $A$ is maximal. The integral domain $B := A/\mathfrak{p}$ satisfies the descending chain condition by hypothesis. Take any $0 \neq x \in B$. Looking at the descending chain $\langle x \rangle \supseteq \langle x^2 \rangle \supseteq \cdots$ allows us to conclude that $\langle x^n \rangle = \langle x^{n+1} \rangle$ for some $n \in \mathbb{N}$, i.e., $x^n \in \langle x^{n+1} \rangle$, i.e., $x^n = x^{n+1}y$ for some $y \in B$. Since $B$ is a domain and $x \neq 0$, we have $xy = 1$, i.e., $x$ is a unit in $B$. It follows that $B$ is a field, i.e., $\mathfrak{p}$ is maximal in $A$.

[only if] A Dedekind domain $A$ satisfies conditions (1) and (2) by definition. In order to prove condition (3) I take a non-zero $A$-ideal $\mathfrak{a}$ and let $B := A/\mathfrak{a}$. Suppose that $\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$ is the factorization of $\mathfrak{a}$. The ideals of $B$ are in one-to-one order-preserving correspondence with the ideals of $A$ containing (i.e., dividing) $\mathfrak{a}$. The only ideals of $A$ dividing $\mathfrak{a}$ are $\mathfrak{p}_1^{f_1} \ldots \mathfrak{p}_r^{f_r}$, where $0 \leqslant f_i \leqslant e_i$ for all $i = 1, \ldots, r$. In particular $B$ contains only finitely many ideals. Therefore every descending chain of ideals of $B$ has to be stationary.

**5.** $K \cong \mathbb{Q}[X]/\langle f(X)\rangle$, where $f(X) := \mathrm{minpoly}_{\omega,\mathbb{Q}}(X) = \Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Consider the polynomial $g(X) := (X-1)f(X) = X^p - 1$. We have $g(X+1) = Xf(X+1) = (X+1)^p - 1 = \left(X^p + \binom{p}{1}X^{p-1} + \binom{p}{2}X^{p-2} + \cdots + \binom{p}{p-1}X + 1\right) - 1$, i.e., $g(X+1) \equiv X^p \pmod p$, i.e., $g(X) \equiv (X-1)^p \pmod p$, i.e., $f(X) \equiv (X-1)^{p-1} \pmod p$. Since $\mathfrak{O}_K = \mathbb{Z}[\omega]$, we can apply the procedure described in Section 4.3 to conclude that $p\mathfrak{O}_k = \mathfrak{q}^{p-1}$, where $\mathfrak{q} = \langle p, \omega - 1\rangle$. Now $0 = f(\omega) = (\omega-1+1)^{p-1} + (\omega-1+1)^{p-2} + \cdots + (\omega-1+1) + 1 = (\omega-1)\alpha + p$ for some $\alpha \in \mathbb{Z}[\omega]$. This implies that $(\omega - 1) \mid p$ in $\mathfrak{O}_K$ and consequently $\mathfrak{q} = \langle \omega - 1\rangle$.

**6.** This is not necessarily true. As an example take $K := \mathbb{Q}(\mathrm{i})$ (so that $\mathfrak{O} = \mathbb{Z}[\mathrm{i}]$), $\mathfrak{a} := \langle 2+\mathrm{i}\rangle$ and $\alpha := 2 - \mathrm{i}$. Then $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\alpha) = 5$, but $(2-\mathrm{i})/(2+\mathrm{i}) = (3/5) - \mathrm{i}(4/5) \notin \mathfrak{O}$, so that $\alpha \notin \mathfrak{a}$.

**7.** Let $\mathfrak{C}$ be an ideal class of $K$. Choose any integral ideal $\mathfrak{c} \in \mathfrak{C}^{-1}$. Then there exists a non-zero integral ideal $\mathfrak{b}$ of $\mathfrak{O}$, such that $\mathfrak{bc}$ is a principal ideal. But then $[\mathfrak{b}] = [\mathfrak{c}]^{-1} \in \mathfrak{C}$. Moreover $\mathfrak{b}$ can be so chosen that $\mathfrak{a} + \mathfrak{b} = \mathfrak{O}$. (See Lemma 4.17.)

**8.** We have $\omega_m = \exp(\mathrm{i}2\pi u/m)$ for some (integer) $u$, $\gcd(u,m) = 1$, and $\omega_n = \exp(\mathrm{i}2\pi v/n)$ for some $v$, $\gcd(v,n) = 1$. Thus $\omega_m\omega_n = \exp(\mathrm{i}2\pi(un+vm)/mn)$ and since $un + vm$ is coprime to $mn$, it follows that $\omega_m\omega_n$ is a primitive $mn$-th root of unity and so $K := \mathbb{Q}(\omega_m, \omega_n) = \mathbb{Q}(\omega_m\omega_n)$ with $[K : \mathbb{Q}] = \phi(m)\phi(n) = \phi(mn)$. The minimal polynomial of $\omega_m\omega_n$ is the $mn$-th cyclotomic polynomial $\Phi_{mn}(X)$. By Exercise 2 it follows that $\mathrm{N}_{K|\mathbb{Q}}(1 - \omega_m\omega_n) = \Phi_{mn}(1)$. Since $mn$ has at least two distinct prime divisors, by the following claim we have $\mathrm{N}_{K|\mathbb{Q}}(1-\omega_m\omega_n) = 1$, i.e., $1 - \omega_m\omega_n$ is a unit in $\mathfrak{O}_K$.

**Claim:** For $k \in \mathbb{N}$, $k \geqslant 2$, we have:

$$\Phi_k(1) = \begin{cases} p & \text{if } k = p^e \text{ for some } p \in \mathbb{P} \text{ and } e \in \mathbb{N}, \\ 1 & \text{otherwise.} \end{cases}$$

*Proof* Let us proceed by induction on $k$. First consider the case $k = p^e$ for some $p \in \mathbb{P}$ and $e \in \mathbb{N}$. Then $\Phi_k(X) = X^{p^{e-1}(p-1)} + X^{p^{e-1}(p-2)} + \cdots + X^{p^{e-1}} + 1$ (as can be easily verified by induction on $e$) and it is immediate that $\Phi_k(1) = p$ in this case. Now let $k = p_1^{e_1} \cdots p_r^{e_r}$ with pairwise distinct primes $p_1, \ldots, p_r$, $r \geqslant 2$, and assume that the result holds for all integers greater than 1 and smaller than $k$. We have

$$\Phi_k(X) = \frac{X^k - 1}{\prod_{\substack{d \mid k \\ 1 \leqslant d < k}} \Phi_d(X)} = \frac{X^{k-1} + X^{k-2} + \cdots + X + 1}{\prod_{\substack{d \mid k \\ 1 < d < k}} \Phi_d(X)},$$

since $\Phi_1(X) = X - 1$. By the induction hypothesis we deduce that

$$\Phi_k(1) = \frac{k}{\left(\prod_{\substack{d \mid k \\ 1<d<k \\ \nu(d)>1}} \Phi_d(1)\right)\left(\Phi_{p_1}(1) \cdots \Phi_{p_1^{e_1}}(1)\right) \cdots \left(\Phi_{p_r}(1) \cdots \Phi_{p_r^{e_r}}(1)\right)} = \frac{k}{p_1^{e_1} \cdots p_r^{e_r}} = 1,$$

where $\nu(d)$ denotes the number of distinct prime divisors of $d$. •

(**Remark:** An immediate corollary to this exercise is that *for co-prime integers* $m > 1$ *and* $n > 1$ *the resultant* $\mathrm{Res}(\Phi_m, \Phi_n)$ *is* 1. For the proof let us write $\mathrm{N}(1-\omega_m\omega_n)$ in a different way. Let $\alpha_1, \ldots, \alpha_{\phi(m)}$ be all the conjugates of $\omega_m$ and $\beta_1, \ldots, \beta_{\phi(n)}$ those of $\omega_n$. One can simply verify that the $\phi(mn) = \phi(m)\phi(n)$ complex numbers $\alpha_i\beta_j$, $1 \leqslant i \leqslant \phi(m)$ and $1 \leqslant j \leqslant \phi(n)$, are all the conjugates of $\omega_m\omega_n$. Therefore all the conjugates of $1 - \omega_m\omega_n$ are $1 - \alpha_i\beta_j$. Consequently $1 = \mathrm{N}(1 - \omega_m\omega_n) = \prod_{i,j}(1 - \alpha_i\beta_j) = \prod_i \left(\alpha_i^{\phi(n)} \prod_j (\alpha_i^{-1} - \beta_j)\right) = \left(\prod_i \alpha_i\right)^{\phi(n)} \left(\prod_i \Phi_n(\alpha_i^{-1})\right)$. Now $\prod_i \alpha_i = \begin{cases} -1 & \text{if } m = 2, \\ +1 & \text{if } m > 2. \end{cases}$ If $m = 2$, then $n \geqslant 3$ and hence $\phi(n)$ is even. In both the cases we have $\left(\prod_i \alpha_i\right)^{\phi(n)} = +1$, i.e., $1 = \prod_i \Phi_n(\alpha_i^{-1}) = \prod_i \Phi_n(\alpha_i) = \mathrm{Res}(\Phi_m, \Phi_n)$.)

**9.** Let us consider the quadratic number field $K := \mathbb{Q}(\sqrt{-D})$. Since $-D \equiv 2, 3 \pmod 4$, it follows that $\mathfrak{O} := \mathfrak{O}_K = \mathbb{Z}[\sqrt{-D}]$. Suppose that there exist integers $x$ and $y$ satisfying $y^2 = x^3 - D$. If a rational prime $p$ divides $\gcd(x, y)$, then $p^2 \mid D$, contrary to the hypothesis that $D$ is square-free; so $\gcd(x, y) = 1$.

We have a factorization in $\mathfrak{O}$ as $(y+\sqrt{-D})(y-\sqrt{-D}) = x^3$, i.e., $\langle y+\sqrt{-D}\rangle\langle y-\sqrt{-D}\rangle = \langle x^3\rangle = \langle x\rangle^3$. I claim that the $\mathfrak{O}$-ideals $\langle y+\sqrt{-D}\rangle$ and $\langle y-\sqrt{-D}\rangle$ are coprime. For the proof assume otherwise, i.e., let a non-zero prime $\mathfrak{O}$-ideal $\mathfrak{p}$ divide both these ideals. Then $\mathfrak{p}$ divides the gcd of the two ideals, which is $\langle y+\sqrt{-D}\rangle + \langle y-\sqrt{-D}\rangle \supseteq \langle 2y\rangle$, i.e., $\mathfrak{p} \mid \langle 2y\rangle = \langle 2\rangle\langle y\rangle$. Now $\mathfrak{p}$ also divides $\langle x\rangle$, and $x$ and $y$ are coprime in $\mathbb{Z}$ (and hence in $\mathfrak{O}$ too). Therefore $\mathfrak{p} \mid \langle 2\rangle$, i.e., $\mathrm{N}(\mathfrak{p}) = 2^i$ for $i = 1$ or $2$. Since $\mathfrak{p} \mid \langle x\rangle$ and hence $\mathrm{N}(\mathfrak{p}) \mid \mathrm{N}(\langle x\rangle) = x^2$, it follows that $x$ must be even, so that $0 \equiv x^3 \equiv y^2 + D \pmod 4$, a contradiction, since $y^2 \equiv 0, 1 \pmod 4$ and $D \equiv 1, 2 \pmod 4$.

Considering unique factorization of ideals we then conclude that $\langle y+\sqrt{-D}\rangle = \mathfrak{a}^3$ and $\langle y-\sqrt{-D}\rangle = \mathfrak{b}^3$ for some relatively prime $\mathfrak{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$. Now $3 \nmid h_K$ and $\mathfrak{a}^3$ is a principal ideal. Therefore $\mathfrak{a}$ itself is principal, i.e., $\mathfrak{a} = \langle a + b\sqrt{-D}\rangle$ for some $a, b \in \mathbb{Z}$, i.e., $y + \sqrt{-D} = \xi(a + b\sqrt{-D})^3$ for some unit $\xi \in \mathfrak{U}_K$. If $\xi = u + v\sqrt{-D}$ (with $u, v \in \mathbb{Z}$), we have $\pm 1 = \mathrm{N}(\xi) = u^2 + Dv^2$, i.e., $u = \pm 1$ and $v = 0$ (since $D > 1$), i.e., $\xi = \pm 1$, i.e., $y + \sqrt{-D} = \pm(a + b\sqrt{-D})^3$, i.e., $\pm y = a^3 - 3ab^2D$ and $\pm 1 = 3a^2b - b^3D = b(3a^2 - b^2D)$. The last equation implies that $b \mid 1$, i.e., $b = \pm 1$, i.e., $D = 3a^2 \pm 1$, a contradiction to the hypothesis that $D$ is not of this form.