CTNT 2018 Exercises for Algebraic Number Theory

Lecture I: Number Fields.

Exercise 1.1. Consider the cyclotomic field $F = \mathbb{Q}(\zeta_p)$ (with $p > 2$ an odd prime and $\zeta_p = e^{2\pi i/p}$). Note that $[F : \mathbb{Q}(\zeta_p)] = p - 1$

(1) What is the minimal polynomial of ζ_p over $\mathbb{Q}$?
(2) What are the embeddings of F?
(3) What is the trace of $a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ for $a_0, \ldots, a_{p-2} \in \mathbb{Q}$?
(4) What is $\mathrm{Nm}_{F/\mathbb{Q}}(\zeta_p - 1)$?

Exercise 1.2. Here is another definition of the trace and norm: pick a basis $e_1, \ldots, e_n$ of the field F as a $\mathbb{Q}$-vector space. Take $\alpha \in F$. Consider multiplication by α as a $\mathbb{Q}$-linear transformation on F (as a $\mathbb{Q}$-vector space). Then this linear transformation with respect to the chosen basis $e_1, \ldots, e_n$ is given by an $n \times n$-matrix with coefficients in $\mathbb{Q}$ we define

$$\mathrm{Tr}'_{F/\mathbb{Q}}(\alpha) = \mathrm{trace}(A), \quad \mathrm{Nm}'_{F/\mathbb{Q}}(\alpha) = \det(A).$$

(1) When $F = \mathbb{Q}(\sqrt{d})$ with d a square-free integer, we choose the basis $\{1, \sqrt{d}\}$. Compute $\mathrm{Tr}'_{F/\mathbb{Q}}(a + b\sqrt{d})$ and $\mathrm{Nm}'_{F/\mathbb{Q}}(a + b\sqrt{d})$ by writing out the corresponding matrix and compute its trace and determinant.
(2) Show that the definition of $\mathrm{Tr}'_{F/\mathbb{Q}}$ and $\mathrm{Nm}'_{F/\mathbb{Q}}$ are independent of the choice of the basis.
(3) Show that when $F = \mathbb{Q}(\alpha)$, the definition of trace and determinant agrees with what we used in the lecture. That is, if $h(x) = x^n + a_1x^{n-1} + \cdots + a_n$ is the minimal polynomial of α, then

$$\mathrm{Tr}'_{F/\mathbb{Q}}(\alpha) = -a_1 \quad \text{and} \quad \mathrm{Nm}'_{F/\mathbb{Q}}(\alpha) = (-1)^n a_n.$$

(Hint: consider the basis given by $1, \alpha, \ldots, \alpha^{n-1}$.)

Exercise 1.3. Verify by definition that for $F = \mathbb{Q}(\sqrt{d})$ with $d \neq 1$ a square-free integer,

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

In each case, what is $\mathrm{disc}(\mathcal{O}_F)$?

Exercise 1.4. Consider $F = \mathbb{Q}(\alpha)$ with α a zero of an irreducible polynomial $h(x) = x^3 + ax + b$ where $a, b \in \mathbb{Z}$.

(1) Show that $\mathrm{disc}(1, \alpha, \alpha^2) = -\mathrm{Nm}_{F/\mathbb{Q}}(f'(\alpha)) = -4a^3 - 27b^2$, where $f'(x)$ is the formal derivative of $f(x)$.
(2) In case when $a = b = -1$, that is $\alpha^3 = \alpha + 1$. Compute $\mathrm{disc}(1, \alpha, \alpha^2)$ using (1) and conclude that $\mathcal{O}_F = \mathbb{Z}[\alpha]$.

Exercise 1.5. Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_F$ be algebraic integers. Use the trick that

$$\det \begin{pmatrix} \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \tau_n(\alpha_1) & \cdots & \tau_n(\alpha_n) \end{pmatrix}^2 = \det \begin{pmatrix} \tau_1(\alpha_1) & \tau_2(\alpha_1) & \cdots & \tau_n(\alpha_1) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_1(\alpha_n) & \tau_2(\alpha_n) & \cdots & \tau_n(\alpha_n) \end{pmatrix} \begin{pmatrix} \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \tau_2(\alpha_1) & \cdots & \tau_2(\alpha_n) \\ \vdots & \ddots & \vdots \\ \tau_n(\alpha_1) & \cdots & \tau_n(\alpha_n) \end{pmatrix}$$

$$= \begin{pmatrix} \mathrm{Tr}_{F/\mathbb{Q}}(\alpha_1^2) & \cdots & \mathrm{Tr}_{F/\mathbb{Q}}(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha_n\alpha_1) & \cdots & \mathrm{Tr}_{F/\mathbb{Q}}(\alpha_n^2) \end{pmatrix}$$

to show that $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

Exercise 1.6. Let F be a number field with r_1 real embeddings $\tau_1, \ldots, \tau_{r_1} : F \hookrightarrow \mathbb{R}$ and r_2 *pairs* of complex embeddings

$$\tau_{r_1+1}, \ldots, \tau_{r_1+2r_2} : F \hookrightarrow \mathbb{C},$$

such that $\tau_{r_1+2i}(x) = \overline{\tau_{r_1+2i-1}(x)}$ for $x \in F$. (In particular, $n = r_1 + 2r_2$.)

(1) Consider the case $F = \mathbb{Q}(\sqrt{-d})$ for $d \in \mathbb{Z}_{>1}$ square-free. Instead of considering the embedding $\tau_1, \tau_2 = \overline{\tau}_1 : F \hookrightarrow \mathbb{C}$, we consider the embedding:

$$\begin{aligned} (\mathrm{Re}(\tau_1), \mathrm{Im}(\tau_1)) : \ F &\hookrightarrow \mathbb{C} \simeq \mathbb{R}^2 \\ a + b\sqrt{-d} &\longmapsto (a, b\sqrt{-d}). \end{aligned}$$

The image of $\mathcal{O}_F$ is a lattice in $\mathbb{R}^2$. Show that the square of the fundamental area of this lattice is $-\frac{1}{4}\mathrm{disc}(\mathcal{O}_F)$. (It might help to think about the case $\mathcal{O}_F = \mathbb{Z}[\sqrt{-d}]$.)

(2) Consider in the general case, the following embedding:

$$\big(\tau_1, \ \ldots, \tau_{r_1}, \ \mathrm{Re}(\tau_{r_1+1}), \ \mathrm{Im}(\tau_{r_1+1}), \ \mathrm{Re}(\tau_{r_1+3}), \ \mathrm{Im}(\tau_{r_1+3}), \ \ldots\big) : \ F \longrightarrow \mathbb{R}^n.$$

Show that the square of the fundamental area of the image of $\mathcal{O}_F$ in $\mathbb{R}^n$ is $(-\frac{1}{4})^{r_2}\mathrm{disc}(\mathcal{O}_F)$. In particular, this implies that $\mathrm{disc}(\mathcal{O}_F)$ has the same sign as $(-1)^{r_2}$.

Lecture II: Factorization of Ideals.

Exercise 2.1. Consider $F = \mathbb{Q}(\sqrt{-39})$ and $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{-39}}{2}]$. As explained in the lecture, we have

$$2 \cdot 5 = \tfrac{1+\sqrt{-39}}{2} \cdot \tfrac{1-\sqrt{-39}}{2}.$$

Check that this can be explained by the ideal factorization:

$$\begin{aligned} (2)(5) &= (2, \tfrac{1+\sqrt{-39}}{2})(2, \tfrac{1-\sqrt{-39}}{2}) \cdot (5, \tfrac{1+\sqrt{-39}}{2})(5, \tfrac{1-\sqrt{-39}}{2}), \\ (\tfrac{1+\sqrt{-39}}{2})(\tfrac{1-\sqrt{-39}}{2}) &= (2, \tfrac{1+\sqrt{-39}}{2})(5, \tfrac{1+\sqrt{-39}}{2}) \cdot (2, \tfrac{1-\sqrt{-39}}{2})(5, \tfrac{1-\sqrt{-39}}{2}). \end{aligned}$$

Exercise 2.2. Consider $F = \mathbb{Q}(\zeta_5)$ for $\zeta_5 = e^{2\pi i/5}$. Accept the fact that $\mathcal{O}_F = \mathbb{Z}[\zeta_5]$ and that the minimal polynomial of ζ_5 is $\frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$.

(1) Give the factorization of $3\mathcal{O}_F$, $5\mathcal{O}_F$, $11\mathcal{O}_F$, and $19\mathcal{O}_F$.
(2) What are the ramification index and inertia degree in each case?

Exercise 2.3. Consider $F = \mathbb{Q}(\sqrt{d})$ with $d \neq 1$ a square-free integer. Prove by explicit computation that a prime p is ramified in F if and only if $p \mid \mathrm{disc}(\mathcal{O}_F)$. (Hint: e.g. when $d \equiv 2, 3 \bmod 4$, the factorization of $p\mathcal{O}_F$ is determined by the polynomial $x^2 - d$ modulo p. The prime $p = 2$ needs to be discussed separately.)

Exercise 2.4. Consider $F = \mathbb{Q}(\sqrt[3]{10})$. Set $\alpha = \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}$.

(1) Show that $\mathrm{disc}(\alpha) = -300 = 3 \cdot 2^2 \cdot 5^2$.
(2) Prove that 2 and 5 ramify in F, by checking that $2\mathbb{Z}[\alpha] = (2, \sqrt[3]{10})^3$ and $5\mathbb{Z}[\alpha] = (5, \sqrt[3]{10})^3$.
(3) Recall that a prime p is ramified in $F/\mathbb{Q}$ if and only if $p \mid \mathrm{disc}(F)$. From this deduce that $\mathcal{O}_F = \mathbb{Z}[\alpha]$.

Exercise 2.5. Consider $F = \mathbb{Q}(\alpha)$ with $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$. Admitting the fact that $2\mathcal{O}_F$ splits completely, we prove that $\mathcal{O}_F$ cannot be generated by one element of $\mathcal{O}_F$.

Suppose not; $\mathcal{O}_F = \mathbb{Z}[\beta]$ for some $\beta \in \mathcal{O}_F$. Let $h(x) \in \mathbb{Z}[x]$ denote the (monic) minimal polynomial of β. Explain why $2\mathcal{O}_F$ splits completely implies that $h(x) \bmod 2$ must splits completely into distinct factors in $\mathbb{F}_2[x]$. From this deduce a contradiction. (Hint: Is there a cubic polynomial over $\mathbb{F}_2$ that splits completely?) Can you generalize this to a degree n number field?

Exercise 2.6. Solve the following question with the given steps: which (positive) integer m is the sum of two squares $x^2 + y^2$ for $x, y \in \mathbb{Z}$? If it is, in how many ways?

(1) Solving $m = x^2 + y^2$ is equivalent to finding an element $x + yi \in \mathbb{Z}[i]$ such that $m = \mathrm{Nm}_{\mathbb{Q}(i)/\mathbb{Q}}(x + yi)$.
(2) Show that every $4k + 1$ type prime p factors in $\mathbb{Z}[i]$ as $p = (u + vi)(u - vi)$ for $u, v \in \mathbb{N}$.
(3) Factor m as the product:

$$m = 2^\lambda \cdot p_1^{\mu_1} \cdots p_r^{\mu_r} \cdot q_1^{\nu_1} \cdots q_s^{\nu_s},$$

where $p_1, \ldots, p_r$ are (distinct) $4k+3$ type primes and $q_1, \ldots, q_s$ are (distinct) $4k+1$ type primes.

Prove that m is the sum of two squares if and only if $\mu_1, \ldots, \mu_r$ are all even numbers. In this case, prove that an element $x+yi \in \mathbb{Z}[i]$ is so that $m = \mathrm{Nm}(x+yi)$ if and only if

$$x + yi = u \cdot (1+i)^\lambda \cdot p_1^{\mu_1/2} \cdots p_r^{\mu_r/2} \cdot (u_1 + v_1 i)^{a_1}(u_1 - v_1 i)^{b_1} \cdots (u_s + v_s i)^{a_s}(u_s - v_s i)^{b_s}$$

where u is a unit (i.e. $u \in \{\pm 1, \pm i\}$, $p_1, \ldots, p_r$ are the (distinct) $4k + 3$ type primes, $q_j = u_j^2 + v_j^2$ for every j, and $\nu_j = a_j + b_j$ for every j.

(4) Make explicit what this means by working out the case when $m = 5 \cdot 13$, when $m = 1105 = 5 \cdot 13 \cdot 17$, and when $m = 2 \cdot 13$.

Lecture III: Ideal Class Groups

Exercise 3.1. In the example $F = \mathbb{Q}(\sqrt{-39})$, for $\alpha = \frac{1+\sqrt{-39}}{2}$, show that $(2, \alpha)^4 = (\alpha+2)$.

Exercise 3.2. Use the Minkowski bound to show the real quadratic field $\mathbb{Q}(\sqrt{d})$ has class number 1 if $d = 2, 3, 6$ and class number 2 if $d = 10$.

Exercise 3.3. Use the Minkowski bound to show the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ has class number 2 if $d = 5, 6$ and class number 4 if $d = 14$.

Exercise 3.4. For an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ with $-d \equiv 2, 3 \bmod 4$ a square-free natural number.

(1) Prove that if an ideal I has norm $m < d$ and m is not a square, then I is not a principal ideal.
(2) So if for any odd prime number $p < d$, $-d$ is a square modulo p, then $\mathbb{Q}(\sqrt{-d})$ is not a PID.
(3) What is the corresponding statement when $-d \equiv 1 \bmod 4$?

We hope to convey through this example that, intuitively, why only finitely many imaginary quadratic fields have class number 1.

Exercise 3.5. Consider $F = \mathbb{Q}(\alpha)$ with α satisfying $\alpha^3 = \alpha + 1$ (per Exercise 1.4(2)). Prove that $\mathcal{O}_F = \mathbb{Z}[\alpha]$ is a PID.

Exercise 3.6. Consider $F = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Accept the fact that $\mathcal{O}_F = \mathbb{Z}[\sqrt{2}, \frac{1+\sqrt{-3}}{2}]$.

(1) Compute the discriminant of $\mathcal{O}_F$.
(2) Prove that $\mathcal{O}_F$ is a PID.
(3) Note that F contains $\mathbb{Q}(\sqrt{-6})$ which is not a PID. This gives an example that a number field with class number > 1 could have a finite extension which has class number 1. Recall that $(2, \sqrt{-6})$ is not a principal ideal in $\mathbb{Z}[\sqrt{-6}]$. Find a principal generator of $(2, \sqrt{-6})$ in $\mathcal{O}_F$.

Lecture IV: Unit Groups.

Exercise 4.1. Let F be a quadratic field and let $\mu(F)$ denote the roots of unity in F. Show that $\mu(F) = \{\pm 1\}$ except when $F = \mathbb{Q}(i)$ (in which case $\mu(F) = \{\pm 1, \pm i\}$) and when $F = \mathbb{Q}(\sqrt{-3})$ (in which case $\mu(F) = \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$).

Moreover, if F is an imaginary quadratic field, $\mathcal{O}_F^\times = \mu(F)$.

Exercise 4.2. The -1 Pell's equation $x^2 - dy^2 = -1$ may not always have solutions.

(1) If $d > 0$ and $d \equiv 3 \bmod 4$ is square-free, show that $x^2 - dy^2 = -1$ has no solution in integers x, y. (Hint: consider modulo 4.) (Remark: this means that in this case, all units of $\mathbb{Z}[\sqrt{d}]$ have norm 1 (as opposed to possibly -1).)
(2) Show $x^2 - dy^2 = -1$ has no solution in integers when $d = 6$, 14, and 22. (Hint: modulo 8.)

Exercise 4.3. Consider a biquadratic field $F = \mathbb{Q}(\sqrt{a}, \sqrt{-b})$ with $a, b > 0$ (implicitly, we assume that $F/\mathbb{Q}$ has degree 4 and has Galois group $(\mathbb{Z}/2\mathbb{Z})^2$; note that F also contains the imaginary quadratic field $\mathbb{Q}(\sqrt{-ab})$.) Assume that F does not contain $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$.
(1) Prove that $\mu(F) = \{\pm 1\}$. (Hint: If $\mu(F)$ contains other roots of unity ζ_n, then $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is a quotient group of $\mathrm{Gal}(F/\mathbb{Q})$.)
(2) Show that $\mathcal{O}_F^\times$ is a subgroup of $\mathcal{O}_{\mathbb{Q}(\sqrt{a})}^\times$ of index at most 2. (Hint: (1) implies that there is a generator $u \in \mathcal{O}_F^\times$ such that $\mathcal{O}_F^\times = \pm u^{\mathbb{Z}}$. Consider the action of complex conjugation u.)
(3) Give an example when $\mathcal{O}_F^\times \neq \mathcal{O}_{\mathbb{Q}(\sqrt{a})}^\times$.

Exercise 4.4. In $\mathbb{Z}[\sqrt[4]{2}]$, show $u = 1 + \sqrt[4]{2}$ and $v = 1 + \sqrt{2}$ are units and they are multiplicatively independent: if $u^a v^b = 1$ for $a, b \in \mathbb{Z}$ then $a = 0$ and $b = 0$.

Exercise 4.5. For a Dirichlet character $\chi : (\mathbb{Z}/8\mathbb{Z})^\times \to \{\pm 1\}$ given by $\chi(1) = \chi(7) = 1$ and $\chi(3) = \chi(5) = -1$. Compute the following L-value:

$$L(\chi, 1) := 1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \frac{1}{13} + \frac{1}{15} + \cdots$$

(Hint: set $f(x) = x - \frac{1}{3}x^3 - \frac{1}{5}x^5 + \frac{1}{7}x^7 + \cdots$, compute $f'(x)$ first, and then find $f(x)$ by integration.) Note that $\ln(\sqrt{2} + 1)$ shows up naturally (and note that $\sqrt{2} + 1$ is the generator of the unit group $\mathbb{Z}[\sqrt{2}]^\times$ and $\mathrm{disc}(\mathbb{Z}[\sqrt{2}]) = 8$).