Number Theory Homework #6 *Spring 2026*

Instructor: *Chan Ieong Kuan*

Solutions by: ***Haoyu Zhu***

Exercises

1 Algebraic Number Theory

1. Exercise 12.9

Solution Set $\sigma_i(\alpha) = \alpha_i$, the conjugate roots of $x^3 + px + q$, and $\alpha_1 = \alpha$. We know

$$\Delta(1, \alpha, \alpha^2) = (-1)^3 N(f'(\alpha)) = (-1) \prod_{i=1}^{3} (3\alpha_i^2 + p).$$

Since $\sum_i \alpha_i = 0$, $\sum_{i<j} \alpha_i\alpha_j = p$, and $\prod_i \alpha_i = -q$, we can expand the product and compute:

$$\prod_{i=1}^{3} (3\alpha_i^2 + p) = 27 \prod_i \alpha_i^2 + 9p \sum_{i<j} \alpha_i^2\alpha_j^2 + 3p^2 \sum_i \alpha_i^2 + p^3.$$

$$\prod_i \alpha_i^2 = (\alpha_1\alpha_2\alpha_3)^2 = (-q)^2 = q^2,$$

$$\sum_i \alpha_i^2 = \big(\sum_i \alpha_i\big)^2 - 2\sum_{i<j} \alpha_i\alpha_j = 0 - 2p = -2p,$$

$$\sum_{i<j} \alpha_i^2\alpha_j^2 = \big(\sum_{i<j} \alpha_i\alpha_j\big)^2 - 2\alpha_1\alpha_2\alpha_3 \sum_i \alpha_i = p^2 - 2(-q) \cdot 0 = p^2.$$

Substitute:

$$\prod_{i=1}^{3} (3\alpha_i^2 + p) = 27q^2 + 9p \cdot p^2 + 3p^2(-2p) + p^3 = 27q^2 + 9p^3 - 6p^3 + p^3 = 4p^3 + 27q^2.$$

Therefore,

$$\Delta(1, \alpha, \alpha^2) = (-1)(4p^3 + 27q^2) = -4p^3 - 27q^2.$$

◀

2. Exercise 12.10

Proof. ($\Rightarrow$) Suppose S is a field. Let $r \in R \subset S$ be nonzero, and then $r^{-1} \in S$, i.e. there exists a monic polynomial with coefficients in R such that:

$$(r^{-1})^n + a_{n-1}(r^{-1})^{n-1} + \cdots + a_0 = 0, \qquad a_i \in R.$$

Multiply by $r^{n-1} \in R$: $r^{-1} + a_{n-1} + a_{n-2}r + \cdots + a_0 r^{n-1} = 0$. Thus $r^{-1} = -(a_{n-1} + a_{n-2}r + \cdots + a_0 r^{n-1}) \in R$. Hence R is a field.

($\Leftarrow$) Now assume R is a field and S is an integral domain. Let $s \in S$ be nonzero. Since S is integral over R, there exists a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$ with $f(s) = 0$. Choose minimal n with $a_0 \neq 0$. As R is a field, a_0 is invertible in $R \subset S$. From $f(s) = 0$, we obtain $s\big(-a_0^{-1}(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1)\big) = 1$, so s has an inverse in S. Thus S is a field. □

3. Exercise 12.28

Lemma 1.1. $\mathcal{O}_F$ is a Dedekind domain, so after localization $\mathcal{O}_{F,P}$ is a discrete valuation ring with $P\mathcal{O}_{F,P}$ the unique nonzero maximal ideal, hence in its Jacobson radical. If $P = P^2$, then $P\mathcal{O}_{F,P} = P^2\mathcal{O}_{F,P} = (P\mathcal{O}_{F,P})^2$. Now $P\mathcal{O}_{F,P}$ is a finitely generated $\mathcal{O}_{F,P}-$module, and $P\mathcal{O}_{F,P}$ is in the Jacobson radical og $\mathcal{O}_{F,P}$. Now we can apply the Nakayama lemma to obtain $P\mathcal{O}_{F,P} = 0$. Contradiction occurs. Therefore, $P \neq P^2$.

Lemma 1.2. For any algebraic integer a, we have $\prod_i (x - \sigma_i(a))$ its minimal monic polynomial with integer coefficients. Therefore, its trace $\sum_i \sigma_i(a) \in \mathbb{Z}$.

Proof. (a) P is prime, hence maximal in $\mathcal{O}_F$, so $P + A = \mathcal{O}_F$. What's more, $P \neq P^2$. Therefore, there exist $a \in A, a \notin P, \pi \in P, \pi \notin P^2$. Then $(a) + P = \mathcal{O}_F$, so $\exists p_0 \in P, a_0 \in \mathcal{O}_F, a_0 \notin P, aa_0 + p_0 = 1$. Consider $aa_0\pi = \pi - p_0\pi \in PA$, since $\pi \notin P^2, \pi p_0 \in P^2$, we obtain $aa_0\pi \notin P^2 \supseteq P^2A$. In conclusion, we find $\alpha \triangleq aa_0\pi$.

In fact, from **proposition 9.2** of *Introduction to commutative algebra* by Atiyah, every non-zero ideal is power of $\mathfrak{m}$ and we can define a valuation $v_p(a)$ for any element a. Therefore, $v_p(a\pi) = v_p(a) + v_p(\pi) = 0 + 1 = 1 < 2$, so $a\pi$ following our construction cannot be contained in P^2A.

(b) $(\alpha\beta)^p \in P^pA^p\mathcal{O}_F \subset P^2A = (p)$, hence $(\alpha\beta)^p \in p\mathcal{O}_F$.

(c) Write $x = \alpha\beta$. Equivalently, we should show that

$$\left(\sum_i \sigma_i(x)\right)^p - \sum_i (\sigma_i(x))^p = \sum_{\sum_i e_i = p} a_I \prod_i (\sigma_i(x))^{e_i} \in p\mathcal{O}_F,$$

where $a_I = \frac{p!}{\prod_i (e_i!)} \in p\mathbb{Z}$. However, $x, x^p \in \mathcal{O}_F$, so $(\sum_i \sigma_i(x))^p - \sum_i (\sigma_i(x))^p \in \mathbb{Z}$. Given a galois extension of F, say L, then $\sigma_i(x) \in \mathcal{O}_L$. Therefore,

$$\sum_{\sum_i e_i = p} a_I \prod_i (\sigma_i(x))^{e_i} \in p\mathcal{O}_L \cap \mathbb{Z} = p\mathbb{Z}.$$

(d) We know that

$$\left(\sum_i \sigma_i(x)\right)^p - \sum_i (\sigma_i(x))^p \in p\mathbb{Z},$$

and $x^p = py$ for some $y \in \mathcal{O}_F$. Therefore, $\sum_i (\sigma_i(x))^p = p \sum_i \sigma_i(y) \in p\mathbb{Z}$, and then $(\sum_i \sigma_i(x))^p \in p\mathbb{Z}$. What's more, the trace of x is an integer, hence in $p\mathbb{Z}$, too.

(e) Given an integral basis $\{\omega_i\}$, we know that $p \mid tr(\alpha\omega_i)$. If $\alpha = \sum_i a_i \omega_i$, we have $\sum_i a_i tr(\omega_i \omega_j) \equiv 0 \pmod p$ for any j. However, $\alpha \notin p\mathcal{O}_F$, i.e. $(a_i)_i \neq (0, 0, \ldots, 0) \pmod p$, so $det(tr(\omega_i\omega_j)) \equiv 0 \pmod p$ by linear matrix theory.

□

2 Dirichlet L-functions

4. Exercise 16.4 ($p = 3$)

Proof. Since $L(1, \chi)$ is a convergent series, we can change the order of summation. $L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{n=0}^{\infty} \frac{1}{3n+1} + \sum_{n=0}^{\infty} \frac{-1}{3n+2} + \sum_{n=1}^{\infty} \frac{0}{3n} = \sum_{n=0}^{\infty} \frac{1}{(3n+1)(3n+2)}$. By Excercise 16.8,

$$\prod_{\chi(n)=-1} (1 - \zeta^n) \prod_{\chi(r)=1} (1 - \zeta^r)^{-1} = \exp\bigl(g(\chi) L(1, \chi)\bigr).$$

Now, $\chi(1) = 1$, $\chi(2) = -1$ and $\zeta = e^{2\pi i/3}$. Then

$$\text{LHS} = \frac{1 - \zeta^2}{1 - \zeta} = e^{i\pi/3}, g(\chi) = i\sqrt{p} = i\sqrt{3}.$$

Hence

$$\exp\bigl(i\sqrt{3}\, L(1, \chi)\bigr) = e^{i\pi/3} \implies i\sqrt{3}\, L(1, \chi) = i\pi/3 + 2\pi i k,\ k \in \mathbb{Z}.$$

Since $L(1, \chi) = \sum_{n=0}^{\infty} \frac{1}{(3n+1)(3n+2)}$ is a positive real number, we obtain $L(1, \chi) = \dfrac{\pi}{3\sqrt{3}}$.

□

5. Exercise 16.8:

Solution We rewrite the left-hand side as a product over all $x \in \mathbb{Z}_p^*$:

$$\prod_{\chi(n)=-1} (1-\zeta^n) \prod_{\chi(r)=1} (1-\zeta^r)^{-1} = \prod_{x=1}^{p-1} (1-\zeta^x)^{-\chi(x)}.$$

Taking logarithms defined by expanding $\log(1-\zeta^x) = -\sum_{k\geq 1} \frac{\zeta^{xk}}{k}$ yields

$$\log(\text{LHS}) = -\sum_{x=1}^{p-1} \chi(x) \log(1-\zeta^x) = \sum_{x=1}^{p-1} \chi(x) \sum_{k=1}^{\infty} \frac{\zeta^{xk}}{k} = \sum_{k=1}^{\infty} \frac{1}{k} \sum_{x=1}^{p-1} \chi(x)\zeta^{xk}.$$

For a prime p and the Legendre symbol χ, the Gauss sum satisfies

$$\sum_{x=1}^{p-1} \chi(x)\zeta^{xk} = \begin{cases} \chi(k)g(\chi), & p \nmid k, \\ 0, & p \mid k. \end{cases}$$

Hence

$$\log(\text{LHS}) = \sum_{\substack{k=1 \\ p\nmid k}}^{\infty} \frac{\chi(k)g(\chi)}{k} = g(\chi) \sum_{\substack{n=1 \\ p\nmid n}}^{\infty} \frac{\chi(n)}{n} = g(\chi)L(1,\chi).$$

Exponentiating gives $\text{LHS} = \exp\big(g(\chi)L(1,\chi)\big)$. ◀

6. Exercise 16.9 ($p = 5$)

Solution By Excercise 16.8,

$$\prod_{\chi(n)=-1} (1-\zeta^n) \prod_{\chi(r)=1} (1-\zeta^r)^{-1} = \exp\big(g(\chi)L(1,\chi)\big).$$

Now $\chi(1) = \chi(4) = 1,\ \chi(2) = \chi(3) = -1$ and $\zeta = e^{2\pi i/5}$. Then

$$\text{LHS} = \frac{(1-\zeta^2)(1-\zeta^3)}{(1-\zeta)(1-\zeta^4)} = \frac{3+\sqrt{5}}{2}, g(\chi) = \sqrt{p} = \sqrt{5}.$$

Since $L(1,\chi)$ is a positive real number in this case, we obtain

$$\exp\big(\sqrt{5}\,L(1,\chi)\big) = \frac{3+\sqrt{5}}{2} \implies L(1,\chi) = \frac{1}{\sqrt{5}} \log \frac{3+\sqrt{5}}{2} = \frac{2}{\sqrt{5}} \log \frac{1+\sqrt{5}}{2}.$$

◀