Set 1.

Please study the following Problems 1-10 by January 18 (Friday).

In Problems 1-10, let X be a compact Hausdorff space and let A be the ring of all $\mathbb{C}$-valued continuous functions on X. We consider how X is reflected in A and how A is reflected in X like the relation of a flower and its image in the water.

For a subset S of X, let $I(S)$ be the ideal $\{f \in A \mid f(p) = 0 \text{ for all } p \in S\}$ of A. For a subset E of A, let $V(E)$ be the closed subset $\{p \in X \mid f(p) = 0 \text{ for all } f \in E\}$ of X.

1. Prove that if S is a subset of X, then $V(I(S)) = \bar{S}$ where $\bar{S}$ is the closure of S.

(You can use the following property of a compact Hausdorff space X. Let C be a closed subset of X and let $p \in X$, $p \notin C$. Then there is $f \in A$ such that $f(p) = 1$ and f has value 0 at any point of S.)

2. Prove that for a subset S of X, S is closed if and only if there is an ideal I of A such that $S = V(I)$.

3. Prove that if I is an ideal of A such that $V(I) = \emptyset$, then $I = A$.

This is not easy to prove. Here is a suggestion for the proof. Note that $\cap_{i=1}^{n} V(f_i) = V(f_1\bar{f}_1 + \cdots + f_n\bar{f}_n)$ for $f_1, \cdots, f_n \in A$, and use the assumption $\cap_{f \in I} V(f) = V(I) = \emptyset$ and the compactness of X. Here $V(f)$ for $f \in A$ means $V(\{f\})$ (i.e. V of the subset $\{f\}$ of A), and $\bar{f}$ denotes the function on X

$$p \mapsto \quad \text{the complex conjugate of } f(p).$$

4. Prove that the map $X \to \max(A)\ ;\ p \mapsto \{f \in A \mid f(p) = 0\}$ is bijective. Here $\max(A)$ denotes the set of all maximal ideals of A.

Suggestion for the proof. To get the surjectivity of this map, apply Problem 3 to a maximal ideal I of A. For the injectivity, use Problem 1.

5. Let $\mathrm{Hom}_{\mathbb{C}}(A, \mathbb{C})$ be the set of all ring homomorphisms over $\mathbb{C}$. Prove that the map

$$X \to \mathrm{Hom}_{\mathbb{C}}(A, \mathbb{C})$$

is bijective.

Here the meaning of "ring homomorphism over $\mathbb{C}$" is the following. Let k be a commutative ring. A commutative ring over k is a commutative ring endowed with a fixed ring homomorphism form k. For commutative rings R_1, R_2 over k, a ring homomorphism $\varphi : R_1 \to R_2$ is called a ring homomorphism over k if the composition $k \to R_1 \overset{\varphi}{\to} R_2$ of φ and the fixed $k \to R_1$ coincides with the fixed $k \to R_2$.

Suggestion for the proof for Problem 5. You can use the fact that the map $X \to \max(A)\ ;\ p \mapsto \{f \in A \mid f(p) = 0\}$ is bijective.

6. Let Y be another compact Hausdorff space and let B be the ring of all $\mathbb{C}$-valued continuous functions on Y. Let $\varphi : A \to B$ be a ring homomorphism over $\mathbb{C}$. Prove that there is a unique continuous map $\Phi : Y \to X$ such that $\varphi(f) = f \circ \Phi$ for any $f \in A$. Here $f \circ \Phi$ denotes the composition $Y \stackrel{\Phi}{\to} X \stackrel{f}{\to} \mathbb{C}$.

(Remark: Using the terminology of category theory, this can be said as follows. The contravariant functor

$$\{\text{Compact Hausdorff spaces}\} \to \{\text{Commutative rings over } \mathbb{C}\} ;$$

$$X \mapsto \{\text{continuous } \mathbb{C}\text{-valued functions on } X\}$$

is fully faithful.)

7. In Problem 6, prove that $\varphi : A \to B$ is injective if and only if $\Phi : Y \to X$ is surjective.

8. In Problem 6, prove that $\varphi : A \to B$ is surjective if and only if $\Phi : Y \to X$ is injective. (You can use the property of a compact Hausdorff space X that a $\mathbb{C}$-valued continuous function on a closed subset C of X extends to a $\mathbb{C}$-valued continuous function on X.)

9. Prove that X is connected if and only if there is no $f \in A$ such that $f^2 = f$, $f \neq 0$, $f \neq 1$.

10. Assume X is a finite set. Prove that $S \mapsto I(S)$ is a bijection from the set of all subsets of X to the set of all ideals of A, and that $J \mapsto V(J)$ (here J is an ideal of A) is the inverse map of this bijection.

Suggestion for the proof. You can use the fact that for a product $A_1 \times A_2$ of commutative rings (the addition and the multiplication are component-wise), any ideal of $A_1 \times A_2$ has the form $I_1 \times I_2$ where I_1 is an ideal of A_1 and I_2 is an ideal of A_2. As a commutative ring, A in Problem 10 is isomorphic to the product of n copies of $\mathbb{C}$ where n is the order of the finite set X.

Set 2.

Please study the following Problems 11–20 by January 25 (Friday).

This time, we consider integer solutions of algebraic equations by thinking about the friends ($\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, $\cdots$) of $\mathbb{Z}$.

In Problems 11-16, we consider integer solutions of algebraic equations like $x^3 = y^2 + 2$. Let m be an even integer such that $m < 0$ and such that m is not divisible by r^2 for any integer $r > 1$. It is known that the integer ring of $\mathbb{Q}(\sqrt{m})$ is $\mathbb{Z}[\sqrt{m}]$.

11. Prove that if p is a prime number which divides m, then $(p, \sqrt{m})$ is a maximal ideal of $\mathbb{Z}[\sqrt{m}]$. (Hint for the proof. Recall that for an ideal I of a commutative ring R, I is a maximal ideal if and only if R/I is a field. By using $\mathbb{Z}[\sqrt{m}] \cong \mathbb{Z}[T]/(T^2 - m)$, where T corresponds to $\sqrt{m}$ in this isomorphism, prove that $\mathbb{Z}[\sqrt{m}]/(p, \sqrt{m})$ is isomorphic to the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.)

In Problems 12-13, let a be an integer and assume that any prime divisor of a is a prime divisor of m. We consider integer solutions of $x^3 = y^2 - a^2 m$ by using the method explained in the course.

12. Assume $x, y \in \mathbb{Z}$, $x^3 = y^2 - a^2 m$. Prove that $(y + a\sqrt{m}) = I^3$ for some non-zero ideal I of $\mathbb{Z}[\sqrt{m}]$.

13. Assume $x, y \in \mathbb{Z}$, $x^3 = y^2 - a^2 m$ and assume that the class number of $\mathbb{Q}(\sqrt{m})$ is not divisible by 3. Prove that $y + a\sqrt{m} = \alpha^3$ for some $\alpha \in \mathbb{Z}[\sqrt{m}]$. (You can use the fact $\mathbb{Z}[\sqrt{m}]^\times = \{\pm 1\}$.)

14. By using the fact the class number of $\mathbb{Q}(\sqrt{-2})$ is 1, prove that all integer solutions of $x^3 = y^2 + 2$ are given by $(x, y) = (3, \pm 5)$.

(Remark. Fermat gave all integer solutions of $x^3 = y^2 + 2$, and also all integer solutions of $x^3 = y^2 + 4$ explained in the course.)

15. By using the fact the class number of $\mathbb{Q}(\sqrt{-6})$ is 2, prove that all integer solutions of $x^3 = y^2 + 54$ are given by $(x, y) = (7, \pm 17)$.

16. By using the fact the class number of $\mathbb{Q}(\sqrt{-14})$ is 4, prove that all integer solutions of $x^3 = y^2 + 56$ are given by $(x, y) = (18, \pm 76)$.

In Problems 17-20, we consider integer solutions of algebraic equations like $x^2 - 2y^2 = \pm 1$.

17. Prove that there is a bijection between the two sets $\mathbb{Z}[\sqrt{2}]^\times$ and $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x^2 - 2y^2 = \pm 1\}$ given by $x + y\sqrt{2} \leftrightarrow (x, y)$ $(x, y \in \mathbb{Z})$.

18. For $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ $(x, y \in \mathbb{Z})$, prove that $x + y\sqrt{2} > 1$ if and only if $x > 0$ and $y > 0$. Using the fact $(x, y) = (1, 1)$ is the smallest integer solution of $x^2 - y^2 = \pm 1$ such that $x > 0$ and $y > 0$, prove that $1 + \sqrt{2}$ is the smallest element of $\mathbb{Z}[\sqrt{2}]^\times$ which is > 1.

19. By using Problems 17 and 18, prove that $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$.

20. Prove that $\mathbb{Z}[\sqrt{3}]^\times = \{\pm(2 + \sqrt{3})^n \mid n \in \mathbb{Z}\}$.

Dear first year students,

One of you told me that Problem 12 of Set 2 is hard. I completely agree because I was already worrying that it was hard when I sent the problem to you. I hope to write a hint. I am sorry if you solved that problem already without a hint.

It seems that it is necessary to prove the following (1).

(1) If $\mathfrak{p}$ is a maximal ideal which contains $2a\sqrt{m}$, $\mathfrak{p}$ coincides with $(p, \sqrt{m})$ for some prime divisor p of m.

It seems that (1) is divided into the following (2) and (3).

(2) If p is a prime divisor of m and if $\mathfrak{p}$ is a maximal ideal which contains p, then $\mathfrak{p} = (p, \sqrt{m})$.

(3) If $\mathfrak{p}$ is a maximal ideal which contains $\sqrt{m}$, then $\mathfrak{p} = (p, \sqrt{m})$ for some prime divisor p of m.

For (2), think about maximal ideals of

$$\mathbb{Z}[\sqrt{m}]/(p) = \mathbb{Z}[T]/(T^2 - m, p) = \mathbb{F}_p[T]/(T^2).$$

For (3), similarly think about maximal ideals of

$$\mathbb{Z}[\sqrt{m}]/(\sqrt{m}) = \mathbb{Z}[T]/(T^2 - m, T).$$

Best regards, Kazuya

Set 3.

Please study the following Problems 21-30 by February 1 (Friday).

This time, we consider problems related to decompositions of prime numbers in the integer ring of a quadratic fields.

A maximal ideal of O_K for a number field K is nothing but a non-zero prime ideal of O_K. In number theory, people usually call a maximal of O_K just a prime ideal, not putting non-zero. I will follow them.

21. Using the uniqueness of the prime factorization in $\mathbb{Z}[i]$, prove that if

$$\tan(\alpha) = 1, \quad \tan(\beta) = 3/2, \quad \tan(\gamma) = 2,$$

then α, β, γ are linearly independent over $\mathbb{Q}$.

22. Let p be a prime number and assume $p \neq 2, 3$. Using $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}$ (a special case of the quadratic reciprocity law), prove the following. If $p \equiv 1, 11 \bmod 12$, (p) in $\mathbb{Z}\sqrt{3}]$ decomposes into the product of two different prime ideals. If $p \equiv 5, 7 \bmod 12$, p is a prime element in $\mathbb{Z}[\sqrt{3}]$.

23. By using the fact $\mathbb{Z}[\sqrt{3}]$ is a PID, prove that for a prime number $p \neq 2, 3$, $p = \pm(x^2 - 3y^2)$ for some $x, y \in \mathbb{Z}$ if $p \equiv 1, 11 \bmod 12$, and that p can not be expressed in that way if $p \equiv 5, 7 \bmod 12$.

24. Let p be a prime number and assume $p \neq 2$. Computing $\left(\frac{-2}{p}\right)$ and using the fact $\mathbb{Z}[\sqrt{-2}]$ is a PID, prove that $p = x^2 + 2y^2$ for some $x, y \in \mathbb{Z}$ if $p \equiv 1, 3 \bmod 8$, and that p can not be expressed in that way if $p \equiv 5, 7 \bmod 8$.

25. Let p be a prime number and assume $p \neq 2$. Computing $\left(\frac{2}{p}\right)$ and using the fact $\mathbb{Z}[\sqrt{2}]$ is a PID, prove that $p = x^2 - 2y^2$ for some $x, y \in \mathbb{Z}$ if $p \equiv 1, 7 \bmod 8$, and that p can not be expressed in that way if $p \equiv 3, 5 \bmod 8$. (You may think that $p = \pm(x^2 - 2y^2)$ appears. That is correct, but improve it to $p = x^2 - 2y^2$ by multiplying $x + y\sqrt{2}$ by the unit $1 + \sqrt{2}$ if necessary.)

26. (Problems 26 and 27 arise from the fact that the part [improve it ....] in Problem 25 does not work for $\mathbb{Z}[\sqrt{3}]$. It is because $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$ whereas $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$.) Let p be a prime number, and assume $p \neq 2, 3$. Prove that if $p = x^2 - 3y^2$ $(x, y \in \mathbb{Z})$, then $p \equiv 1 \bmod 12$. Prove that if $p = -(x^2 - 3y^2)$ $(x, y \in \mathbb{Z})$, then $p \equiv 11 \bmod 12$.

27. By using 22 and 26, prove that for a prime number $p \neq 2, 3$, $p = x^2 - 3y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \bmod 12$.

28. Let p be a prime number and assume $p \neq 2, 5$. The quadratic reciprocity law tells that $\left(\frac{-5}{p}\right)$ is 1 if $p \equiv 1, 3, 7, 9 \bmod 20$ and is -1 if $p \equiv 11, 13, 17, 19 \bmod 20$. One thing which did not appear in Problems 21–27 is that the integer ring $\mathbb{Z}[\sqrt{-5}]$ of $\mathbb{Q}(\sqrt{-5})$ is not a PID. In Problem 28, assume $p \equiv 1, 3, 7, 9 \bmod 20$ and write $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ for a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\sqrt{-5}]$. Here $\bar{\mathfrak{p}}$ is the complex conjugate of $\mathfrak{p}$. In

this Problem 28, assume further that $\mathfrak{p}$ is a principal ideal. Prove that $p = \alpha\bar{\alpha}$ for some $\alpha \in \mathbb{Z}[\sqrt{-5}]$. Prove that $p \equiv 1, 9 \bmod 20$.

29. As in Problem 28, assume $p \equiv 1, 3, 7, 9 \bmod 20$ and write $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, and assume this time that $\mathfrak{p}$ is not a principal ideal. Let $\mathfrak{a} = (2, 1+\sqrt{-5})$ which is not a principal ideal. Note that by the fact the class number of $\mathbb{Q}(\sqrt{-5})$ is 2, we see that $\mathfrak{a}\mathfrak{p}$ is a principal ideal. By using the fact $(2) = \mathfrak{a}\bar{\mathfrak{a}}$ $(= \mathfrak{a}^2)$, prove that $2p = \alpha\bar{\alpha}$ for some $\alpha \in \mathbb{Z}[\sqrt{-5}]$. Prove that $p \equiv 3, 7 \bmod 20$.

30. By using Problems 28 and 29, prove that for a prime number $p \neq 2, 5$, $p = x^2 + 5y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 9 \bmod 20$.

Set 4

Please study the following Problems 31-40 by February 8 (Friday).

As in my course on February 1 (Friday), for a finitely generated commutative ring A over $\mathbb{Z}$, the Hasse zeta function of A is defined by

$$\zeta_A(s) = \prod_m (1 - \sharp(A/m)^{-s})^{-1}$$

where m ranges over all maximal ideals of A.

31. Let $\mathbb{F}_q$ be a finite field consisting of q elements. As an analogue of the formula for Rieman's zeta function

$$\zeta(s) = \zeta_{\mathbb{Z}}(s) = \prod_p (1 - p^{-s})^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

in which p ranges over all prime numbers, prove

$$\zeta_{\mathbb{F}_q[T]}(s) = \sum_f \frac{1}{\sharp(\mathbb{F}_q[T]/(f))^s}$$

where f ranges over all monic polynomials in $\mathbb{F}_q[T]$. By using it, prove that

$$\zeta_{\mathbb{F}_q[T]}(s) = \frac{1}{1 - q^{1-s}}.$$

Remark. The analogue of Riemann's hypothesis for $\zeta_{\mathbb{F}_q[T]}(s)$ is not interesting, for this zeta function has no zero. In homeworks Set 5, you will see that the analogues of Riemann's hypothesis for $\zeta_A(s)$ are interesting for some friends A of $\mathbb{F}_q[T]$.

Before I present Problem 32, I write something about $\zeta(s)$. For the fact there exist infinitely many prime numbers, Euler gave the following analytic proof by using two presentations (the additive presentation and the product presentation) of $\zeta(s)$. We can prove that when $s > 1$ tends to 1, then $\sum_{n=1}^{\infty} n^{-s}$ tends to ∞. If there were only finite number of prime numbers, when $s > 1$ tends to 1, $\prod_p (1 - p^{-s})^{-1}$ should converge to $\prod_p (1 - p^{-1})^{-1}$ and would not tend to ∞. Thus we have a contradiction and hence there are infinitely many prime numbers.

32. By using Problem 31 and by using the method of Euler, prove that there are infinitely many irreducible monic polynomials in $\mathbb{F}_q[T]$.

33. For a commutative ring A which is finitely generated over $\mathbb{Z}$, prove that $\zeta_{A[T_1,\ldots,T_n]}(s) = \zeta_A(s - n)$. Here $\zeta_A(s)$ denotes the Hasse zeta function of A.

(This is a homework in algebra (not in analysis), and so please do not worry here about the convergence of the infinite product. Precisely speaking, this problem has sense if we already know that the (usually infinite) product $\zeta_A(s)$ converges

absolutely when $Re(s)$ is sufficiently large.) Suggestion of the proof. Use induction on n and the result on $\zeta_{\mathbb{F}_q[T]}(s)$ in Problem 31.

34. By using Problem 33, prove that for any commutative ring A which is finitely generated over $\mathbb{Z}$, $\zeta_A(s)$ (as a product) converges absolutely when $Re(s)$ is sufficiently large.

Since this is a homework in algebra, it is fine that analytic arguments are not perfectly precise.

Preparation for Problems 35.

A Dirichlet character is a homomorphism $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ where N is an integer ≥ 1. For a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, the Dirichlet L-function $L(s, \chi)$ is defined as

$$L(s, \chi) = \sum_n \chi(n) n^{-s}$$

where n ranges over all integers ≥ 1 which are coprime to N ($\chi(n)$ means $\chi(n \bmod N)$). This infinite series converges when the real part $Re(s)$ of the complex number s is > 1. In the case $N = 1$ and χ is the trivial homomorphism, $L(s, \chi)$ is Riemann's zeta function $\zeta(s) = \sum_{n=1}^\infty n^{-s}$ and so Dirichlet L-function is a generalization of Riemann zeta function. Like Riemann zeta function, Dirichlet L-function has the presentation as a product over prime numbers

$$L(s, \chi) = \prod_p (1 - \chi(p) p^{-s})^{-1}$$

where p ranges over all prime numbers which do not divide N. $L(s, \chi)$ has an analytic continuation to the whole $\mathbb{C}$ as a meromorphic function, and is holomorphic at any $s \neq 1$. (In fact, if χ is not the trivial homomorphism, then $L(s, \chi)$ is holomorphic also at $s = 1$.)

Example. In the case $N = 1$ and $\chi : (\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3 \bmod 4\} \to \mathbb{C}^\times$ is given by $\chi(1) = 1$ and $\chi(3) = -1$, we have

$$L(s, \chi) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \dots .$$

We consider an analogue of Dirichlet L function for $\mathbb{F}_q[T]$. Let $g \in \mathbb{F}_q[T]$, $g \neq 0$, let $\chi : (\mathbb{F}_q[T]/(g))^\times \to \mathbb{C}^\times$ be a homomorphism, let $c \in \mathbb{C}^\times$, and consider

$$(**) \qquad L_c(s, \chi) = \sum_f \chi(f) \cdot c^{\deg(f)} \cdot \sharp(\mathbb{F}_q[T]/(f))^{-s}$$

where f ranges over all monic polynomials in $\mathbb{F}_q[T]$ which are coprime to g, and deg means the degree. In the case $c = 1$, we will denote $L_c(s, \chi)$ just by $L(s, \chi)$.

We have the presentation $L_c(s, \chi) = \prod_h (1 - \chi(h) \cdot c^{\deg(h)} \cdot \sharp(\mathbb{F}_q[T]/(h))^{-s})^{-1}$ as product, where h ranges over all monic irreducible polynomials in $\mathbb{F}_q[T]$ which do not divide g.

35. In the above (**), consider the case $g = T$ and χ is not the trivial homomorphism. Prove $L_c(s, \chi) = 1$.

Suggestion for the proof. Prove that if $d \geq 1$, $\sum_{a_1,\ldots,a_d \in \mathbb{F}_q} \chi(T^d + a_1 T^{d-1} + \cdots + a_d) = 0$.

The fact there are infinitely many prime numbers p such that $p \equiv 3 \bmod 4$ is proved as follows by using Dirichlet L-function. Consider the Dirichlet L-function $L(s, \chi)$ where χ is as in the above Example before Problem 35. If there were only finitely many prime numbers p such that $p \equiv 3 \bmod 4$, in the product presentation of $L(s, \chi)$, almost all factors $(1 - \chi(p)p^{-s})^{-1}$ (called the Euler factor at p) should be $(1 - p^{-s})^{-1}$, that is, $\zeta(s)$ and $L(s, \chi)$ would have the same Euler factors at almost all p. Since $\zeta(s)$ diverges to ∞ when $s > 1$ tends to 1, $L(s, \chi)$ should diverge to ∞ when $s > 1$ tends to 1. But it can be seen that when $s > 1$ and $s \to 1$, $L(s, \chi) = 1 - 1/3^s + 1/5^s - 1/7^s + 1/9^s - 1/11^s + \cdots$ converges to $1 - 1/3 + 1/5 - 1/7 + 1/9 - 1/11 + \cdots = \pi/4 < \infty$. Contradiction. Hence there are infinitely many prime numbers p such that $p \equiv 3 \bmod 4$. (The fact there are infinitely many prime numbers such that $p \equiv 1 \bmod 4$ can be also proved by using this $L(s, \chi)$.)

36. By using Problem 35, prove that there are infinitely many irreducible monic polynomials $f \in \mathbb{F}_3[T]$ whose constant term is $2 \in \mathbb{F}_3$.

37. Prove that in the above (**), if g is of degree n and χ is not the trivial homomorphism, $L_c(s, \chi)$ is a polynomial of q^{-s} of degree $< n$.

38. By using the formula $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ (p is a prime number $\neq 2$) which appears in the story of quadratic reciprocity law and by considering maximal ideals of $\mathbb{Z}[i]/(p) = \mathbb{Z}[T]/(T^2 + 1, p) = \mathbb{F}_p[T]/(T^2 + 1)$ for each prime number p, prove that

$$\zeta_{\mathbb{Z}[i]}(s) = \zeta(s)L(s, \chi)$$

where $\zeta(s)$ is Riemann zeta function and χ is as in the above Example before Problem 35.

Preparation for Problem 39, 40.

The quadratic reciprocity law has the following analogue for the polynomial ring $\mathbb{F}_q[T]$ over a finite field $\mathbb{F}_q$ of q elements whose characteristic is not 2. This is one example of the mysterious analogies between numbers and polynomials.

Let $f, g \in \mathbb{F}_q[T]$ be irreducible monic polynomials and assume $f \neq g$. Then

$$\left(\frac{g}{f}\right) = \left(\frac{f}{g}\right) \cdot (-1)^{\frac{q-1}{2} \cdot \deg(f)\deg(g)}.$$

Here for $a \in \mathbb{F}_q[T]$ which is not divisible by f, $\left(\frac{a}{f}\right)$ is defined to be 1 if the image of a in the field $\mathbb{F}_q[T]/(f)$ is r^2 for some element r of $\mathbb{F}_q[T]/(f)$, and is defined to be -1 otherwise. (We have $\left(\frac{ab}{f}\right) = \left(\frac{a}{f}\right)\left(\frac{b}{f}\right)$ for $a, b \in \mathbb{F}_q[T]$ which are not divisible by f.)

39. By using the above analogue of quadratic reciprocity law, prove that

$$\zeta_{\mathbb{F}_5[T,\sqrt{T^3+1}]}(s) = \zeta_{\mathbb{F}_5[T]}(s)L(s,\chi),$$

where χ is the homomorphism $(\mathbb{F}_5[T]/(T^3+1))^\times \to \mathbb{C}^\times$ defined by

$$\chi(f \bmod T^3+1) = \big(\frac{f}{T+1}\big)\big(\frac{f}{T^2-T+1}\big).$$

40. Let $\mathbb{F}_q$ be a finite field of characteristic $\neq 2$ of order q, let g be a monic polynomial in $\mathbb{F}_q[T]$ of degree $n \geq 1$ which is not divisible by h^2 for any element $h \in \mathbb{F}_q[T]$ of degree ≥ 1, and let $A = \mathbb{F}_q[T, \sqrt{g}]$. By using Problem 37 and the above analogue of quadratic reciprocity law, prove that the Hasse zeta function of A has the shape

$$\zeta_A(s) = \zeta_{\mathbb{F}_q[T]}(s)L_c(s,\chi)$$

for some homomorphism $(\mathbb{F}_q[T]/(g))^\times \to \{\pm 1\} \subset \mathbb{C}^\times$ and for some $c \in \{\pm 1\}$, and prove that

$$\zeta_A(s) = \frac{\text{a polynomial of } q^{-s} \text{ of degree} < n}{1-q^{1-s}}.$$

1. Some of you had a difficulty in Problem 37. It is proved as follows. It is sufficient to prove the following Claim.

Claim. Let $g \in \mathbb{F}_q[T]$ be of degree $n \geq 1$ and let $\chi : (\mathbb{F}_q[T]/(g))^\times \to \mathbb{C}^\times$ be a non-trivial homomorphism. Then for any $m \geq n$, we have

$$\sum_{a_0,\ldots,a_{m-1} \in \mathbb{F}_q} \chi(T^m + a_{m-1}T^{m-1} + \cdots + a_0) = 0.$$

Here $\chi(f)$ denotes $\chi(f \bmod g)$ if f is coprime to g, and denotes 0 otherwise.

We use the following two Lemmas.

Lemma 1. For any finite group G and for any non-trivial homomorphism $\chi : G \to \mathbb{C}^\times$, we have $\sum_{a \in G} \chi(a) = 0$.

Proof of Lemma 1. Take $b \in G$ such that $\chi(b) \neq 1$. Then $\sum_{a \in G} \chi(a) = \sum_{a \in G} \chi(ab) = \chi(b) \sum_{a \in G} \chi(a)$. This shows $\sum_{a \in G} \chi(a) = 0$.

Lemma 2. For $m \geq n$, the homomorphism of additive groups

$$(\mathbb{F}_q)^m \to \mathbb{F}_q[T]/(g) \ ; \ (a_0, \ldots, a_{m-1}) \mapsto \sum_{i=0}^{m-1} a_i T^i \bmod g$$

is surjective.

Proof of Lemma 2. The case $m = n$ is well known (in that case, the map is bijective). The general case follows from this case.

Proof of Claim. By applying Lemma 1 to the multiplicative group $(\mathbb{F}_q[T]/(g))^\times$, we have $\sum_{h \in (\mathbb{F}_q[T]/(g))^\times} \chi(h) = 0$. Let k be the order of the kernel of the homomorphism of Lemma 2. By Lemma 2, the map

$$\nu : (\mathbb{F}_q)^m \to \mathbb{F}_q[T]/(g) \ ; \ (a_0, \ldots, a_{m-1}) \mapsto T^m + a_{m-1}T^{m-1} + \cdots + a_0 \bmod g$$

is surjective and for any element h of $\mathbb{F}_q[T]/(g)$, the inverse image of h in $(\mathbb{F}_q)^m$ under ν has k elements. Hence

$$\sum_{a_0,\ldots,a_{m-1} \in \mathbb{F}_q} \chi(T^m + a_{m-1}T^{m-1} + \cdots + a_0) = k \cdot \sum_{h \in (\mathbb{F}_q[T]/(g))^\times} \chi(h) = 0.$$

2. I forgot in the class to compare the following (1) and (2). This (2) is a nice example of Langlands correspondence.

(1) $\zeta_{\mathbb{Z}[i]}(s) = \zeta(s)L(s,\chi)$,

(2) $\zeta_{\mathbb{Z}[\sqrt[3]{2}]}(s) = \zeta(s)L(s,f)$.

(1) appeared in Homeworks: χ in (1) is a Dirichlet character $(\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times$ defined by $\chi(1) = 1$, $\chi(3) = -1$. This (1) tells that a prime number $p \neq 2$ decomposes into two in $\mathbb{Z}[i]$ if and only if $p \equiv 1 \bmod 4$.

In (2),

$$f(z) = \eta(6z)(18z) = q\prod_{n=1}^{\infty}(1-q^{6n})(1-q^{18n}) \qquad (q = e^{2\pi iz})$$

and

$$L(s,f) = \sum_{n=1}^{\infty} a_n n^{-s}$$

with a_n determined by

$$q\prod_{n=1}^{\infty}(1-q^{6n})(1-q^{18n}) = \sum_{n=1}^{\infty} a_n q^n$$

$$= q - q^7 - q^{13} - q^{19} + q^{25} + 2q^{31} - q^{37} + 2q^{43} - q^{61} - q^{67} - q^{73} - q^{79} + q^{91} - q^{97} - q^{103}...$$

(The proof of (2) is very hard and can not be given here.) This (2) tells that for a prime number $p \neq 2, 3$, (p) in $\mathbb{Z}[\sqrt[3]{2}]$ decomposes into a product of three maximal ideals if and only if $a_p = 2$. (It is not very hard to see that (2) implies this, but I do not explain it here.) For example, 31 decomposes into three in $\mathbb{Z}[\sqrt[3]{2}]$ as $31 = (3 + \sqrt[3]{2}^2)(3 + 3\sqrt[3]{2} + \sqrt[3]{2}^2)(3 - 3\sqrt[3]{2} + \sqrt[3]{2}^2)$.

This f is a modular form and this is an example of Langlands correspondence between arithmetic and modular forms. Langlands correspondence tells, roughly speaking, that Hasse zeta functions are expressed by zeta functions of modular forms. (Dirichlet character is regarded as a special case of a modular form).

Set 5.

Please study the following Problems 41–50 by February 15 (Friday).

In Problems 41–43, you have examples of analogues of Riemann's hypothesis for friends (like $\mathbb{F}_5[T, \sqrt{T^3+1}]$) of $\mathbb{F}_q[T]$.

Problems 44–46 are about analogues of quadratic reciprocity for $\mathbb{F}_q[T]$.

Problems 47–50 are standard problems on commutative ring theory.

41. Let $A = \mathbb{F}_5[T, \sqrt{T^3+1}]$. By using Problem 39, prove that

$$\zeta_A(s) = \frac{1+5^{1-2s}}{1-5^{1-s}}.$$

Prove Riemann hypothesis for this zeta function.

Comment for the proof. I am afraid that you may waste your precious time just to compute $\chi(f)$ for χ in Problem 39. So I write here the result of my computation. For a monic polynomial f in $\mathbb{F}_5[T]$ of degree < 3 which is coprime to T^3+1, $\chi(f)$ is as follows.

$$\chi(1) = 1,$$
$$\chi(T) = 1, \quad \chi(T+2) = -1, \quad \chi(T+3) = 1, \quad \chi(T+4) = -1,$$
$$\chi(T^2) = 1, \quad \chi(T^2+1) = -1, \quad \chi(T^2+2) = -1, \quad \chi(T^2+3) = 1,$$
$$\chi(T^2+T+1) = 1, \quad \chi(T^2+T+2) = 1, \quad \chi(T^2+T+3) = 1, \quad \chi(T^2+T+4) = 1,$$
$$\chi(T^2+2T) = -1, \quad \chi(T^2+2T+2) = -1, \quad \chi(T^2+2T+3) = -1, \quad \chi(T^2+2T+4) = 1,$$
$$\chi(T^2+3T) = 1, \quad \chi(T^2+3T+1) = 1, \quad \chi(T^2+3T+3) = -1, \quad \chi(T^2+3T+4) = 1,$$
$$\chi(T^2+4T) = -1, \quad \chi(T^2+4T+2) = 1, \quad \chi(T^2+4T+4) = 1.$$

42. Let $A = \mathbb{F}_3[T, \sqrt{T(T-1)(T-2)}]$. Prove that

$$\zeta_A(s) = \zeta_{\mathbb{F}_q[T]}(s) L_{-1}(s,\chi) = \frac{1+3^{1-2s}}{1-3^{1-s}},$$

where χ is the homomorphism $(\mathbb{F}_3[T]/(g))^\times \to \mathbb{C}^\times$ with $g = T(T-1)(T-2)$ defined by

$$\chi(f \bmod T(T-1)(T-2)) = \big(\frac{f}{T}\big)\big(\frac{f}{T-1}\big)\big(\frac{f}{T-2}\big)$$

and $L_{-1}(s,\chi)$ is as in (**) before Problem 35.

Prove Riemann hypothesis for this zeta function.

Comment for the proof. I am a little afraid that you waste your precious time just for the computation of $\chi(f)$ for Problem 42. But this time there are only four

monic polynomials in $\mathbb{F}_3[T]$ of degree < 3 which are coprime to $T(T-1)(T-2)$, so the computation should be not so terrible. They are

$$1, \quad T^2+1, \quad T^2+T+2, \quad T^2+2T+2.$$

43. Let $A = \mathbb{F}_5[T, \sqrt{T(T-1)(T-2)}]$. Prove that

$$\zeta_A(s) = \frac{1+2\cdot 5^{-s}+5^{1-2s}}{1-5^{1-s}}.$$

Prove Riemann hypothesis for this zeta function.

Comment for the proof. I am again afraid that you waste your precious time just for the computation of $\chi(f)$ where $\chi : (\mathbb{F}_5[T]/(g))^\times \to \mathbb{C}^\times$ with $g = T(T-1)(T-2)$ is defined by

$$\chi(f \bmod T(T-1)(T+1)) = \big(\frac{f}{T}\big)\big(\frac{f}{T-1}\big)\big(\frac{f}{T+1}\big).$$

For a monic polynomial f in $\mathbb{F}_5[T]$ of degree < 3 which is coprime to $T(T-1)(T+1)$, $\chi(f)$ is as follows.

$$\chi(1) = 1,$$
$$\chi(T+2) = 1, \quad \chi(T+3) = 1,$$
$$\chi(T^2+1) = 1, \quad \chi(T^2+2) = -1, \quad \chi(T^2+3) = -1,$$
$$\chi(T^2+T+1) = -1, \quad \chi(T^2+T+2) = 1, \quad \chi(T^2+T+4) = 1,$$
$$\chi(T^2+2T+3) = 1, \quad \chi(T^2+2T+4) = 1,,$$
$$\chi(T^2+3T+3) = 1, \quad \chi(T^2+3T+4) = 1,$$
$$\chi(T^2+4T+1) = -1, \quad \chi(T^2+4T+2) = 1, \quad \chi(T^2+4T+4) = 1.$$

44. Let k be a commutative field. For monic polynomials $f, g \in k[T]$ which are coprime, let $[\frac{g}{f}] \in k^\times$ be the image of

$$g \bmod f \in (k[T]/(f))^\times$$

under the norm map $(k[T]/(f))^\times \to k^\times$. Prove

$$[\frac{g}{f}] = [\frac{f}{g}] \cdot (-1)^{\deg(f)\deg(g)}.$$

Here for a commutative ring A over k which is finite dimensional as a k-vector space, the norm map $N : A \to k$ is defined as follows. For $a \in A$, $N(a)$ is the determinant of the k-linear map $A \to A\ ;\ x \mapsto ax$. In the case A is a field, $N : A \to k$ is the norm map which appears in the text book of field theory. If A is a field and is

a Galois extension of k, $N(a) = \prod_{\sigma \in G} \sigma(a)$ where G is the Galois group $\mathrm{Gal}(A/k)$. To prove 44, I suggest to reduce the problem to the case k is an algebraically closed field, and write $f = (T - a_1) \cdots (T - a_m)$ and $g = (T - b_1) \cdots (T - b_n)$, and suggest to prove that $[\frac{g}{f}]$ is equal to $\prod_{1 \leq i \leq m, 1 \leq j \leq n} (a_i - b_j)$.

45. Let $\mathbb{F}_q$ be a finite field of characteristic $\neq 2$ of order q. By using Problem 44, prove the analogue of the quadratic reciprocity law

$$\left(\frac{g}{f}\right) = \left(\frac{f}{g}\right) \cdot (-1)^{\frac{q-1}{2} \cdot \deg(f) \deg(g)}$$

for monic irreducible polynomials $f, g \in \mathbb{F}_q[T]$ such that $f \neq g$.

Suggestions for the proof. It may be helpful to use the following facts. (1) For a finite field k of characteristic not 2, $k^\times/(k^\times)^2$ is of order 2. Here $(k^\times)^2 = \{x^2 \mid x \in k^\times\}$. (2) For a finite field k and for a finite field K which is an extension of k, the norm map $K^\times \to k^\times$ is surjective and induces an isomorphism $K^\times/(K^\times)^2 \stackrel{\cong}{\to} k^\times/(k^\times)^2$.

46. Let $\mathbb{F}_q$ be a finite field, let $n \geq 1$ be an integer, and assume that $q - 1$ is divisible by $2n$. By using 44, prove the following reciprocity law for n-th powers.

If f and g are monic polynomials over $\mathbb{F}_q$ such that $f \neq g$, $f \bmod g$ is an n-th power in the field $\mathbb{F}_q[T]/(g)$ if and only if $g \bmod f$ is an n-th power in the field $\mathbb{F}_q[T]/(f)$.

Grothendieck introduced the notation $\mathrm{Spec}(A)$ for the set of all prime ideals of a commutative ring A, for it remained him of the spectrum of a linear operator. Before he came to algebraic geometry, Grothendieck studied linear operators on infinite dimensional vector spaces.

47. Let $M_n(\mathbb{C})$ be the ring of all (n, n)-matrices over $\mathbb{C}$ and let $\varphi \in M_n(\mathbb{C})$. Let A be the commutative subring of $M_n(\mathbb{C})$ over $\mathbb{C}$ generated over $\mathbb{C}$ by φ. That is,

$$A = \{a_0 + a_1\varphi + a_2\varphi^2 + \cdots + a_n\varphi^n \mid n \geq 0, a_i \in \mathbb{C}\}.$$

Prove that there is a bijection between $\mathrm{Spec}(A)$ and the set of all eigen values of φ.

(The set of all eigen values of φ is called the spectrum of φ.)

In the following Problems 48, 49, 50, we compare what happens for

(a) (X, A) where X is a compact Hausdorff space and A is the ring of $\mathbb{C}$-valued continuous functions on X

and what happens for

(b) (X, A) where A is any commutative ring and $X = \mathrm{Spec}(A)$.

We have the following facts (a1)–(a3) for (X, A) in (a).

(a1) For $f \in A$, f is invertible if and only if $f(x) \neq 0$ for any $x \in X$.

(a2) (This appeared in Problem 1.) For a subset S of X, let $I(S)$ be the ideal $\{f \in A \mid f(x) = 0 \text{ for any } x \in S\}$ of A. For an ideal J of A, let $V(J)$ be the closed subset $\{x \in X \mid f(x) = 0 \text{ for any } f \in J\}$ of X. Then for any subset S of X, $V(I(S))$ coincides with the closure of S.

(a3) Let Y and Z be closed subsets of X. Assume $Y \cap Z = \emptyset$. Then there is a $\mathbb{C}$-valued continuous function f on X such that $f(x) = 0$ for any $x \in Y$ and $f(x) = 1$ for any $x \in Z$.

In the following Problems 48, 49, 50, we consider the analogue of (a1), (a2), (a3) for (X, A) in (b), respectively. For the Problems 48 and 50, you may use the fact that if I is an ideal of a commutative ring A such that $I \neq A$, then there is a maximal ideal m of A such that $I \subset m$.

48. Let (X, A) be as in the above (b). Let $f \in A$. Prove that the following conditions (i)–(iii) are equivalent.

(i) f is invertible.

(ii) $f(\mathfrak{p}) \neq 0$ for any $\mathfrak{p} \in \mathrm{Spec}(A)$.

(iii) $f(\mathfrak{p}) \neq 0$ for any $\mathfrak{p} \in \max(A)$.

Here as in the course, $f(\mathfrak{p})$ for $\mathfrak{p} \in \mathrm{Spec}(A)$ denotes the image of f in the residue field of $\mathfrak{p}$. (The residue field of $\mathfrak{p}$ = the field of fractions $Q(A/\mathfrak{p})$ of the integral domain $A/\mathfrak{p}$.)

49. Let (X, A) be as in the above (b). For a subset S of X, let $I(S)$ be the ideal $\{f \in A \mid f(x) = 0 \text{ for any } x \in S\}$ of A. For an ideal J of A, let $V(J)$ be the subset $\{x \in X \mid f(x) = 0 \text{ for any } f \in J\}$ of X. Recall that as in the course, Zariski topology on X is defined by taking all subsets of X of the form $V(J)$ (for ideals J of A) as closed sets. Prove that for any subset S of X, $V(I(S))$ coincides with the closure of S for Zariski topology.

50. Let (X, A) be as in the above (b). Let I and J be ideals of A. Assume $V(I) \cap V(J) = \emptyset$. Prove that $I + J = A$. Prove that there is $f \in A$ such that $f(x) = 0$ for any $x \in V(I)$ and $f(x) = 1$ for any $x \in V(J)$.

Set 6.

Please study the following Problems 51–60 by February 22 (Friday).

The following fact about Noetherian property may be useful for Problem 51. For a commutative ring A, the following (i) and (ii) are equivalent. (i) A is Noetherian. (ii) For any sequence $I_1, I_2, I_3, \dots$ of ideals of A such that $I_1 \subset I_2 \subset I_3 \subset \dots$, there is $n \geq 1$ such that $I_n = I_{n+1} = I_{n+2} = \dots$. The proof of $(i) \Rightarrow (ii)$ is that the ideal $I := \cup_{n \geq 1} I_n$ is finitely generated by the Noetherian assumption, and the finite generators should belong to some I_n for n big enough, and $I = I_n$ and hence $I_n = I_{n+1} = I_{n+2} = \dots$. I omit the proof of $(ii) \Rightarrow (i)$.

51. Let A be a Noetherian integral domain. Let f be a prime element of A (this means that $f \neq 0$ and the ideal (f) of A is a prime ideal). Prove that there is no prime ideal $\mathfrak{p}$ of A such that $0 \subsetneq \mathfrak{p} \subsetneq (f)$.

A suggestion for the proof: Assume such $\mathfrak{p}$ exists. Take a non-zero element g of $\mathfrak{p}$. By using the fact $f \notin \mathfrak{p}$ and by some argument, get $g = g_1 f$ for some $g_1 \in A$, $g_1 = g_2 f$ for some $g_2 \in A$, $g_2 = g_3 f$ for some $g_3 \in A$, $\dots$, and use the Noetherian property of A looking at the ideals $(g) \subset (g_1) \subset (g_2)$, $\dots$ of A.

52. Let A be a unique factorization domain (UFD; see below). Let $\mathfrak{p}$ be a prime ideal of A. Assume that there is no prime ideal $\mathfrak{q}$ of A such that $(0) \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$. Prove that $\mathfrak{p} = (f)$ for some prime element f of A.

A suggestion for the proof. Take a non-zero element of $\mathfrak{p}$ and consider the prime factorization of it.

Remark. This is just a remark concerning UFD. For a non-zero element a of an integral domain A, the following conditions (i) and (ii) need not coincide. (i) a is a prime element (in the sense written in Problem 51). (ii) $a \notin A^\times$ and a can not be written as bc with $b, c \in A$ such that $b \notin A^\times$ and $c \notin A^\times$. (i) implies (ii) but (ii) need not imply (i). If a non-zero element a of A is written in the form $a = u\pi_1 \dots \pi_n$ with $u \in A^\times$ and with elements π_i of A satisfying (ii), we do not have any uniqueness of such expression of a. But if π_i in this expression are prime elements, this expression of a is unique up to replacements of π_i by $v_i \pi_i$ for units v_i and changes of the order of $\pi_1, \dots, \pi_n$ in the presentation. An integral domain is called UFD if any non-zero element of A is written in the form $u\pi_1 \dots \pi_r$ where $u \in A^\times$ and π_i are prime elements.

53. In the polynomial ring $k[T_1, \dots, T_n]$ in n variables over a field k, the ideals $\mathfrak{p}_i = (T_1, \dots, T_i)$ $(i = 0, 1, \dots, n)$ are prime ideals. ($\mathfrak{p}_0$ means the ideal (0). You do not need prove that they are prime ideals.) Prove that for each $i = 0, 1, \dots, n-1$, there is no prime ideal $\mathfrak{q}$ of A such that $\mathfrak{p}_i \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}_{i+1}$.

Hint. Apply Problem 51 to $A = k[T_1, \dots, T_n]/\mathfrak{p}_i \cong k[T_{i+1}, \dots, T_n]$ and $f = T_{i+1}$.

Let A be the ring of polynomial functions on the algebraic set $X = \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3 + 1\}$. We have an isomorphism $\mathbb{C}[T_1, T_2]/(T_2^2 - T_1^3 - 1) \stackrel{\cong}{\to} A$ by

sending T_1 (resp. T_2) to the function x (resp. y) on X which has value x (resp. y) at $(x, y) \in X$. In the course, I will tell (without proof) the following. A is not PID, but the local ring of A at any prime ideal is PID. In the following Problems 54-56, let $\mathfrak{p}$ be the maximal ideal $\{f \in A \mid f(0,1) = 0\}$ of A. Note that we have $\mathfrak{p} = (x, y-1)$ and that $(y-1)(y+1) = x^3$.

54. Note that any element f of A is written in the form $f_0(y) + f_1(y)x + f_2(y)x^2$, where $f_i(y)$ $(i = 0, 1, 2)$ are polynomials in y. For $i = 0, 1, 2$, let m_i be the $(y-1)$-adic order of $f_i(y)$. (This means that in the case $f_i(y) \neq 0$, $f_i(y)$ is divisible by $(y-1)^{m_i}$ but not divisible by $(y-1)^{m_i+1}$. In the case $f_i(y) = 0$, m_i is defined to be ∞.) Let $m = \min\{3m_i + i \mid i = 0, 1, 2\}$. Prove that if $f \neq 0$, in the local ring $A_{\mathfrak{p}}$ of A at $\mathfrak{p}$, f is x^m times a unit.

55. Let the notation be as in Problem 54. Prove that any non-zero ideal of $A_{\mathfrak{p}}$ is written in the form (x^m) for some $m \geq 0$, and hence $A_{\mathfrak{p}}$ is a PID.

Recall that we have the Taylor expansion

$$(1+x)^a = \sum_{n=0}^{\infty} \binom{a}{n} x^n$$

for $x \in \mathbb{C}$ such that $|x| < 1$, where

$$\binom{a}{0} = 1,\ \binom{a}{1} = a,\ \binom{a}{2} = \frac{a(a-1)}{2},\ \binom{a}{n} = \frac{a(a-1)\dots(a-(n-1))}{n!}.$$

In the case $a = 1/m$ $(m \geq 1)$, this gives an m-th root of $1 + x$. For example,

$$(1+x)^{1/2} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \dots.$$

56. Consider the ring homomorphism $h : A \to \mathbb{C}[[T]]$ over $\mathbb{C}$ which sends x to T and y to $\sum_{n=0}^{\infty} \binom{1/2}{n} T^{3n} = 1 + \frac{1}{2}T^3 - \frac{1}{8}T^6 + \dots$. Prove that h induces a ring homomorphism $A_{\mathfrak{p}} \to \mathbb{C}[[T]]$. Prove that for any $n \geq 1$, the two arrows in

$$\mathbb{C}[T]/(T^n) \to A/\mathfrak{p}^n \cong A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^n = A_{\mathfrak{p}}/x^n A_{\mathfrak{p}} \to \mathbb{C}[[T]]/(T^n) \cong \mathbb{C}[T]/(T^n)$$

are isomorphisms. Here the first arrow is the ring homomorphism over $\mathbb{C}$ which sends T to the class of x, and the second arrow is the ring homomorphism induced by h. Obtain an isomorphism

$$\varprojlim_n A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^n \cong \mathbb{C}[[T]].$$

57. Prove that for any $n \geq 1$, the canonical ring homomorphism $\mathbb{Z}/5^n\mathbb{Z} \to \mathbb{Z}[i]/(2-i)^n$ is an isomorphism. By taking $\varprojlim_n$, deduce that $\mathbb{Z}_5 := \varprojlim_n \mathbb{Z}/5^n\mathbb{Z}$ contains a square root of -1.

58. (Here assume that you already know that $\mathbb{Z}_5$ has a square root of -1.) Prove that there are two ring homomorphisms $\mathbb{Z}[i] \to \mathbb{Z}_5$. (You can use the fact $\mathbb{Z}_5$ is an integral domain.) Show that the inverse image of $5\mathbb{Z}_5 \subset \mathbb{Z}_5$ under one homomorphism is $(2-i) \subset \mathbb{Z}[i]$, and the inverse image of $5\mathbb{Z}_5$ under the other homomorphism is $(2+i) \subset \mathbb{Z}[i]$.

The following is a complement to the story of Taylor expansion written before Problem 56.

For a prime number p and for a rational number a which belongs to $\mathbb{Z}_{(p)} = \{\frac{r}{m} \mid r, m \in \mathbb{Z}, p \not| m\}$, it is known that $\binom{a}{n} \in \mathbb{Z}_{(p)}$ for any $n \geq 0$. For $m \geq 1$ which is prime to p and for $x \in p\mathbb{Z}_p$, an m-th root of $1+x$ in $\mathbb{Z}_p$ is obtained as $\sum_{n=0}^{\infty} \binom{1/m}{n} x^n$. (You do not need to prove these.) The case $p=5$, $m=2$ and $x=-5/4$ of this implies that a square root of $1-5/4 = -1/2^2$ exists in $\mathbb{Z}_5$ and hence a square root of -1 exists in $\mathbb{Z}_5$.

59. Obtain a square root 68 mod $\mathbb{Z}/5^3\mathbb{Z}$ of $-1 = 2^2(1-\frac{5}{4})$ in $\mathbb{Z}/5^3\mathbb{Z}$ by applying the above Taylor expansion of $(1-5/4)^{1/2}$.

(In the computation, if $1/4$ appears, a good method is to expand it as $1/4 = -1/(1-5) = -1-5-5^2-\dots$.)

Note that for a sequence a_n $(n = 1, 2, 3, \dots)$ of rational numbers, for a prime number p, and for $c \in \mathbb{Q}$, a_n converges to c in the p-adic number field $\mathbb{Q}_p$ if and only if the p-adic order $\mathrm{ord}_p(a_n - c)$ tends to ∞.

60. Prove that $1-(2/3)^{n!}$ (resp. $1-6^{n!}$) $(n = 1, 2, 3, \dots)$ converges to 0 in $\mathbb{Q}_p$ for any prime number $p \neq 2, 3$, and converges to 1 in $\mathbb{Q}_2$ and in $\mathbb{R}$ (resp. in $\mathbb{Q}_2$ and in $\mathbb{Q}_3$).

Set 7. Please study the following Problems 61–70 by March 1 (Friday).
This time, you prove quadratic reciprocity law and related things.

61. Let K be a commutative field whose characteristic is not 2 and which contains a primitive 8-th root ζ_8 of 1 (a primitive n-th root of 1 is an element α such that $\alpha^n = 1$ and $\alpha^i \neq 1$ for $1 \leq i < n$).
Prove that $\zeta_8 + \zeta_8^{-1}$ is a square root of 2.

62. Let p be a prime number which is not 2. In Problem 61, take the algebraic closure of $\mathbb{F}_p$ as K. By using the fact $\mathbb{F}_p = \{x \in K \mid x^p = x\}$ and by using Problem 61, prove the formula

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

that is, a square root of 2 exists in $\mathbb{F}_p$ if and only if $p \equiv 1, 7 \bmod 8$ and does not exist if $p \equiv 3, 5 \bmod 8$.

63. Let K be a commutative field whose characteristic is not 3 and which contains a primitive cubic root ζ_3 of 1. Prove that $\zeta_3 - \zeta_3^2$ is a square root of -3. Let p be a prime number which is not $2, 3$. By taking the algebraic closure of $\mathbb{F}_p$ as K and using the fact $\mathbb{F}_p = \{x \in K \mid x^p = x\}$, prove that $\left(\frac{-3}{p}\right)$ is 1 if and only if $p \equiv 1 \bmod 3$.

The following Problems 64 and 65 are preparations for Problem 66 which is a generalization of Problem 63.

64. Let $N \geq 1$ be an integer, let K be a commutative field, and assume that K contains a primitive N-th root ζ_N of 1. For a function $f : \mathbb{Z}/N\mathbb{Z} \to K$, define the Fourier transform $\mathcal{F}(f)$ of f as the function $\mathbb{Z}/N\mathbb{Z} \to K$ defined by

$$(\mathcal{F}(f))(x) = \sum_{y \in \mathbb{Z}/N\mathbb{Z}} f(y)\zeta_N^{xy}.$$

(This is an analogue of the Fourier transform of a function on $\mathbb{R}$.) Let $g = \mathcal{F}(\mathcal{F}(f))$. Prove $g(x) = Nf(-x)$.

65. In Problem 64, in the case N is a prime number q and $f : \mathbb{F}_q = \mathbb{Z}/q\mathbb{Z} \to K$ is defined by $f(x) = \left(\frac{x}{q}\right)$ if $x \neq 0$ and $f(0) = 0$, prove that $\mathcal{F}(f) = G \cdot f$ where $G = \sum_{a \in \mathbb{F}_q^\times} \left(\frac{a}{q}\right)\zeta_q^a$.

66. Let K be a commutative field and let q be a prime number which is different from 2. Assume that the characteristic of K is not $2, q$, and assume that K contains a primitive q-th root ζ_q of 1. Let $q^* = q$ if $q \equiv 1 \bmod 4$, and let $q^* = -q$ if $q \equiv 3 \bmod 4$. Using Problems 64 and 65, prove that

$$\sum_{a \in \mathbb{F}_q^\times} \left(\frac{a}{q}\right)\zeta_q^a \quad \text{is a square root of } q^*.$$

(For Problems 66 and 67, please use the fact $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ freely.)

67. Let p and q be prime number which are not 2 and assume $p \neq q$. In Problem 66, take the algebraic closure of $\mathbb{F}_p$ as K. By using the fact $\mathbb{F}_p = \{x \in K \mid x^p = x\}$ and by using Problem 66, prove the formula

$$(\frac{q^*}{p}) = (\frac{p}{q}).$$

From this, deduce the quadratic reciprocity law

$$(\frac{q}{p}) = (\frac{p}{q}) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

68. By using Problem 64 and Problem 65 taking the algebraic closure of $\mathbb{Q}$ as K, prove that if L is a quadratic field (an extension of $\mathbb{Q}$ of degree 2), then $L \subset \mathbb{Q}(\zeta_N)$ for some $N \geq 1$. Here ζ_N denotes a primitive N-th root of 1.

69. Let K be a commutative field whose characteristic is not 7 and which contains a primitive 7-th root ζ_7 of 1. Prove that for $a = 1, 2, 3$, $\zeta_7^a + \zeta_7^{-a}$ are solutions of $x^3 + x^2 - 2x - 1 = 0$.

Let p be a prime number which is not 7. By taking the algebraic closure of $\mathbb{F}_p$ as K and by using the fact $\mathbb{F}_p = \{x \in K \mid x^p = x\}$, prove that $x^3 + x^2 - 2x - 1 = 0$ has a solution in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \bmod 7$.

70. Let p be a prime number which is not 7. Let $F = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ and let O_F be the integer ring of F. Prove that if $p \equiv \pm 1 \bmod 7$, there are three maximal ideals $\mathfrak{p}$ of O_F such that $pO_F \subset \mathfrak{p}$. Prove that for other p, pO_F is a maximal ideal.

(Please use the fact

$$\mathbb{Z}[T]/(T^3 + T^2 - 2T - 1) \stackrel{\cong}{\to} O_F \ ; \ T \mapsto \zeta_7 + \zeta_7^{-1}. \ )$$