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 $\mathbb{C}[T_1, T_2]/(T_2^2 - T_1^3 - 1) \overset{\cong}{\to} A$ 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 $\begin{pmatrix} a \\ n \end{pmatrix} \in \mathbb{Z}_{(p)}$ 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 $\sum_{n=0}^{\infty} \begin{pmatrix} 1/m \\ n \end{pmatrix} x^n$. (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 $\mathbb{Q}_3$).