CHAPTER

Set Theory and Number Theory

Page 4, line 18: (b) for $n \geq 2$, the truth of P(ℓ) for all $\ell < n$ implies the truth of P(n).

Page 35, line 26: $\cdots, \forall\, a \in \mathbb{Q} \backslash \{0\}$.

Page 38, line 14: $\cdots$. Let $a \neq b, D(a,b) = \epsilon$.

Page 39, line 12:

$$a - tp^{\ell} = p^{\ell}(\frac{m}{n} - t) = p^{\ell}(\frac{m - nt}{n}) = p^{\ell+\ell'}\frac{m'}{n},\ \ p \nmid m'$$
$$D_p(a, tp^{\ell}) = qp^{-\ell-\ell'} < p^{-\ell}$$

Page 39, line 15: $\cdots$ we find a power series expansion of $a = \sum_{i=\ell}^{\infty} t_i p^i$

Page 39, line 20:

$$D(-\frac{1}{6}, 3^{-1} + 1 + 3 + 3^2 + \cdots + 3^n) = 3^{-n-1} \to 0$$

CHAPTER

Group Theory

Page 48, line 22: $\cdots$ which satisfies $a^n = e$

Page 59, lines 26-28:

$$\eta_a(x,y) = ((x+a)', (y+ca)'), \qquad \forall\ (x,y) \in T_2$$

where $(x+a)'$ is the unique real number which satisfies $0 \le (x+a)' < 1, (x+a)-(x+a)' \in \mathbb{Z}$.

Page 60, line 13: Find $\mathrm{Orb}(B)$ for all $B \in O(n,\mathbb{R})$.

Page 60, line 17: (11) Let the group $O(n,\mathbb{R})$ act on the set $Symm(n,\mathbb{R})$ of all real symmetric matrices

Page 60, line 19:

$$A(S) = ASA^{-1}, \qquad \text{where } A \in O(n,\mathbb{R}),\ T \in Symm(n,\mathbb{R})$$

Page 63, line 31:

$$\theta = n\theta_0 + r, \qquad 0 \le r < \theta_0$$

Page 67, line 2: $g_1(-1) * g * g_1$ is obviously surjective. $\cdots$

Page 67, line 8:

$$2 - \frac{2}{n} = \sum_{\text{orbits}} (1 - \frac{v_s}{n}) = \sum_{\text{orbits}} (1 - \frac{1}{n_s}) \tag{1}$$

Page 67, line 10:

$$n_s = o(\mathrm{Stab(s)}) \ge 2$$

Page 70, line 16: Similar to part (5), let us view s_3 as the north pole. Since $v_{s_3} = 12$, then there are 12

Page 71, lines 18-19:

$$\mathbf{G} = \{x \mapsto \frac{ax+b}{cx+d} : det\begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \ne 0\}$$

Let $\mathbf{T}= \{0,1,\infty\}$. Find $\mathrm{Stab}(\mathbf{T})$.

Page 71, line 21: $(\mathbb{Z} \times \mathbb{Z})$.

Page 72, line 10: $\mathrm{Card(class)} \le \mathrm{Card}(\mathbf{G}^{(1)})$ for any conjugate class of $\mathbf{G}$.

Page 74, line 30:

$$\neq (0,2) = \rho_{90}((2,0)) = \rho_{90} * \beta_{(1,0)}((1,0))$$

Page 75, line 15: $(2,5)(3,4)$.

page 78, line 4: $g_1, g_2 \in$ G with

Page 78, line 9: Moreover, $e' = \rho(e) \in$ **H'**, **H'**$\neq \emptyset$, therefore, **H'** is a subgroup.

Page 78, lines 11-12: $\mathbf{F} \neq \emptyset$. Let $g_1, g_2 \in \mathbf{F}$. Then we have

$$\rho(g_1 * g_2^{-1}) = \rho(g_1) * \rho(g_2^{-1}) = \rho(g_1) * \rho(g_2)^{-1} \in \textbf{F'}$$

Page 79, line 26: $\cdots$ subgroup of **G'** and **H** the pre-image of **H'**. The induced

Page 82, line 18:

$$g_1^{-1} * g_2(s) = h(s) = s$$

Page 83, line 29: see that $\sigma(1) = [m]_n$ must generate $\mathbb{Z}_n$. Therefore we must have the following with

Page 83, line 34: $\mathbf{Aut}(\mathbb{Z}_n)$ and $\pi(\sigma) = [m]_n$. □

page 84, line 17: *Proof* Let $g \in G, g_1 \in \mathbf{Inn(G)}$ and $\sigma \in \mathbf{Aut(G)}$. Then we have

Page 84, line 23: (2) Prove that $\mathbf{Aut}(\mathbb{Q})$=$\mathbb{Q}^*$.

Page 86, line 5: normal subgroup $\mathbf{G}_1$. Let $\mathbf{G}^*$ be $\mathbf{G}/\mathbf{G}_1$. Then o($\mathbf{G}^* = p^{n-1}$ and $\cdots$

Page 87, line 11: It is clear that o(**H**)=Card(**H**(a))$\leq$ Card(A)= p^n. □

Page 87, line 21:

$$g * \mathbf{H} * g^{-1} = \mathrm{Stab}(g * \mathbf{H}), \qquad \forall\, g \in \mathbf{G}$$

Page 100, line 28: (7) Let p be a prime factor of a positive integer n with $2 < p < n$. $\dots$

CHAPTER

Polynomials

Page 102, line 16: (3) Distributive law: for any $a, b, c \in \mathbf{K}$, we have

Page 103, line 5: distributive law, we have

Page 104, line 24:

$$u_3 = c_1 + c_3 + c_4 + c_7$$

Page 105, line 21: and there is the multiplicative unity 1, namely $1 \cdot a = a \cdot 1 = a$ for all element $a \in \mathbf{R}$.

Page 105, line 22: (3) Distributive law: for any $a, b, c \in \mathbf{R}$, we have

Page 105, lines 29-30: that it is not required the existence of the multiplicative unity 1. In this case the ring in our definition will be called *a ring with unity*. We shall use the term *ring without unity*

Page 106, line 2: existence of multiplicative unity. For instance, $2\mathbb{Z}$ is a ring without unity.

Page 107, line 1: (4) Prove that $\mathbf{FL(n,}\ \mathbb{R}\mathbf{)}$ is not a commutative ring.

Page 107, line 22: $\cdots$ associative and if there is a unity. Let $\mathbf{R}$ be a ring and

Page 108, lines 20-21: (1) It is easy to see that $\mathbf{R}[x]$ is a ring. The unity for summation 0 for $\mathbf{R}$ is the unity for summation for $\mathbf{R}[x]$. The unity for multiplication 1 is the unity for multiplication for $\mathbf{R}[x]$.

Page 108, line 22: (2) Let $\mathbb{Z}_+$ be the semi-group (Cf Exercise 10, §1) of all $\cdots$

Page 111, lines 20-21:*Proof* It follows from the preceding theorem that if $\mathrm{f}(x)$, $\mathrm{g}(x)$ are non-zero, then $\deg(\mathrm{f}(x)\ \mathrm{g}(x)) \geq 0$, and hence $\mathrm{f}(x)\ \mathrm{g}(x) \neq 0$. ∎

Page 115, line 6:

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m, \qquad b_m \neq 0$$

Page 117, line 9: the rings $\mathbf{K}[x_1, x_2, \cdots, x_n]$. For this purpose, let us introduce,

Page 119, line 2:

$$\alpha_i(x) \equiv 1 \ (\mathrm{mod}\ (x - b_i)), \qquad \alpha_i(x) \equiv 0 \ (\mathrm{mod}\ (x - b_j)) \quad \forall\ j \neq i$$

Page 119, line 10:

$$f(x) \equiv a_i \ (\mathrm{mod}\ (x - b_i)) \quad \forall\ i \quad i.e, \quad f(b_i) = a_i$$

Page 120, line 3: $\cdots$ then the relation $\alpha_1 = \delta_2\alpha_2 = \delta_2\delta_1\alpha_1$ implies $(1-\delta_2\delta_1)\alpha_1 = \alpha_1$ implies $\delta_2\delta_1 = 1$.

Page 121, lines 19-20:

$$\beta = \epsilon_2 \prod \pi_i^{m_i}, \qquad \gamma = \epsilon_3 \prod \pi_i^{n_i}$$
$$\pi\gamma = \epsilon_3\pi \prod \pi^{n_i} = \alpha\beta = \epsilon_1\epsilon_2 \prod \pi_i^{\ell_i} \prod \pi_i^{m_i}$$

Page 121, line 27:

$$\pi_1 \mid \alpha = \epsilon\chi_1(\chi_1^{n_1-1}\prod_{j>1}\chi_j^{n_j})$$

Page 121, line 29:

$$\pi_1 \mid \chi_1 \text{ or } \pi_1 \mid (\chi_1^{n_1-1}\prod_{j>1}\chi_j^{n_j})$$

Page 122, lines 1-2: If $\pi_1 \nmid \chi_1$, then we have $\pi_1 \mid \chi_2(\chi_2^{n_2-1}\prod_{j>2}\chi_j^{n_j})$, namely

$$\pi_1 \mid \chi_2 \text{ or } \pi_1 \mid (\prod_{j>2}\chi_j^{n_j})$$

Page 122, line 14: $\alpha_0, \alpha_1, \cdots, \alpha_n$ of $f(x)$. If deg$(f(x))\geq 1$ and $c(f(x))$ is the set of all units, then $\cdots$

Page 124, lines 1-2:

Theorem 3.9. *Let* **D** *be an integral domain such that every element can be written as a product of irreducible elements. Then every non-zero polynomial* $f(x) \in \mathbf{D}[x]$ *can be written as a product of irreducible elements in* $\mathbf{D}[x]$.

Page 126, line 23: Theorem 3.7., it suffices to show that every irreducible element in $\mathbf{D}[x_n]$ is prime. $\cdots$

Page 129, line 6: $\cdots$ a_i is *nilpotent*, namely there is m_i such that $a_i^{m_i} = 0$, for all $i > 0$.

Page 129, line 12-14: (6) Let $a_1, a_2, \cdots, a_n$ be distinct integers. Prove the following polynomial $f(x)$ is irreducible in $\mathbb{Q}[x]$,

$$f(x) = (\prod_{i=1}^{n}(x-a_i)^2) + 1$$

Page 144, line 19:

$$(A) = \begin{cases} \{0\}, & if A = \emptyset \\ \{\sum_{finite} r_i a_i : r_i \in R, a_i \in A\}, & otherwise \end{cases}$$

Page 144, line 23: that **K**= $\mathbb{Q}$, or $\mathbb{R}$, or $\mathbb{C}$. Let $\mathbf{A} = \{f_i(x_1, \cdots, x_n)\} \subset K[x_1, \cdots, x_n]$ be $\cdots$

Page 146, line 17: (3) $\rho(1) = 1'$, where 1 and $1'$ are unities of **R** and **R'** respectively.

Page 147, line 6: (2) Let the map χ: **R**$\rightarrow$ **R/I** be defined as $\chi(r) = [r]$. Then $\chi \cdots$

Page 147, lines 25-26:

$$\begin{aligned} &= [\rho(r_1 + r_2)] = [\rho(r_1) + \rho(r_2)] \\ &= [\rho(r_1)] + [\rho(r_2)] \end{aligned}$$

Page 150, line 10: (1) In our definition of rings, we assume that there is a unity 1. Let $a = 1 \cdots$

Page 151, line 18: *Theorem (Dedekind & Hasse)* $\cdots$

Page 151, line 20: there exist $u, v \in \mathbf{R}$ with $0 < N(va - ub) < N(a)$, then **R** is a *P.I.D.*.

Page 151, lines 23-24: $\cdots$, then we have $u, v \in \mathbf{R}$ with $0 < N(va - ub) < N(a)$. Note that $va - ub \in I$. Therefore, it is impossible and $a \mid b$. $\square$

Page 151, line 26: Let a be any element in $I \setminus \{0\}$ such that $N(a)$ is minimal. $\cdots$

Page 151, line 29: $\cdots$ Note that the previous inequality is equivalence to $N(u(b/a) - v) < 1$.

Page 151, line 33:

$$u(b/a) - v = (x + y\sqrt{-19})(s + r\sqrt{-19})/z - (q - t\sqrt{-19})$$

Page 152, line 2:

$$N(u(b/a) - v) = (\ell^2 + 19)/z^2 < 1$$

Page 156, line 2:

$$d_p(p) = 1, \qquad d_i(p) \equiv 0(\ mod\ p), \qquad c_i(p) \in \mathbb{Z}$$

Page 156, line 28:

$$f(x, y) = x^2 + y^2 - 1 = 0$$

Page 158, line 26: (ii) Let I be a proper ideal in $\mathbf{C}([a, b])$. Then $\cdots$

Page 159, line 3: (15) Let D be a multiplicative set in $\cdots$

Page 159, line 5: (16) Let **R** be a Noetherian integral domain and D a multiplicative set. $\cdots$

CHAPTER

Linear Algebra

Page 173, lines 6 & 7:

$$\begin{aligned} L'(D) &= (D - a_1)^{m_1} \prod_{j>1} (D - a_j)^{m_j+1} \\ &= \prod_{j>1} (D - a_j)^{m_j+1} (D - a_1)^{m_1} \end{aligned}$$

Page 176, line 5:

subset $R \subset S$, $R \supset W$ and a bijective map $\rho : R \to S'$ with $\cdots$

Page 177, lines 17 & 19:

$$s' \notin [\overline{T}] = \text{ the subspace generated by } \overline{T}.$$

$$[\overline{T}] \neq \mathbf{V} = [S]$$

Page 178, line 2:

$$(1) \qquad as + \sum_{finite} a_i t_i + \sum_{finite} b_j t'_j, \qquad t_i \in \overline{T},\ t'_j \in \S' \backslash \overline{T}'$$

CHAPTER

Polynomial in One Variable and Field Theory

Page 255, line 9:

$$\lim_{x \to \infty} f(x) = \infty$$

Page 257, line 8: (4) Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in \mathbb{Z}[x]$ with $a_n \neq 0$. Suppose $\cdots$

Page 257, line 13:

$$g(x) = \sum_{j=0}^{n} \binom{n}{j} a_j x^{n-j}$$

Page 257, line 25: a **K**-*injection*. If σ is an isomorphism. Then σ is called a **K**-*isomorphism*.

Page 259, line 14: Since $\mathbf{K}[\alpha] \subset \mathbf{L}$, then it is an integral domain. It follows $\cdots$

Page 264, line 30: $\triangle oab \sim \triangle cad$. If we let $\overline{oa} = \alpha$, $\overline{ca} = 1$, and $cd = \beta$, then we have the product $\cdots$

Page 270, line 6:

$$[\mathbf{K}(x) : \mathbf{K}(\frac{f(x)}{g(x)})] = n$$

Page 270, line 16: (7) Prove that $[\mathbb{Q}[e^{2\pi i/8}] : \mathbb{Q}[i]] = 2$.

Page 271, line 3: exists an integer $n \neq 0$ such that $n\alpha$ is an algebraic integer.

Page 272, line 8: Let $f(x)$ be an irreducible element in $\mathbf{K}[x]$. Assume **L** is an extension of **K** such that there is a root α of $f(x)$ in **L**. Let **L'** be an

Page 279, line 24: Therefore $\varphi_n(x) \in \mathbb{Z}[x]$.

Page 281, lines 29-30: (3) Let **K** be a finite field of 2^n elements. Show that a polynomial $f(x) \in \mathbb{Z}_2[x]$ of degree n is primitive if and only if $f(x)$ satisfies the following two

Page 282, line 18: root of an irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree m. $\cdots$

Page 282, line 26:

$$\mathbf{K} \cap \mathbb{R} = \mathbb{Q}[e^{2\pi i/p} + e^{-2\pi i/p}]$$

Page 286, line 9:

$$\mathbf{KL}^p = \{\sum_{i=1}^{n} k_i \ell_i^p : k_i \in \mathbf{K}, \ell_i \in \mathbf{L}.\}$$

Page 291, line 13: (7) Let $\mathbf{L} \supset \mathbf{R} \supset \mathbf{K}$ be field extensions. Suppose that **L** is $\cdots$

Page 291, line 15: (8) Let $\mathbf{L} \supset \mathbf{R} \supset \mathbf{K}$ be field extensions. Suppose that **L** is $\cdots$

Page 304, line 2: of **L**. Let **S** be an extension of **K** in Ω . Then the composition, $\mathbf{L}\cdot\mathbf{S}$, is a Galois $\cdots$

Page 304, line 20: $\cdots$ group $G(R/S)$ is a subgroup of the multiplicative group $\mathbb{Z}_n^* =$

Page 307, line 20: **Definition 5.19** If there exists a chain of radical extensions as follows,

Page 309, line 2: cyclic group of order n, then $f(x)$ can be solved by radicals.

Page 310, lines 3-8: Let $\mathbf{R}=\mathbf{K}_1[\beta_1]$. Then **R** is a radical extension of $\mathbf{K}_1$.

(5) We claim $\mathbf{R}=\mathbf{K}_2$. Note then our theorem is established. It is clear that $\beta_1 \in \mathbf{K}_2$, and $\mathbf{R} \subset \mathbf{K}_2$. On the other hand, none of the σ^j's are the identity map on **R**, therefore, we have

$$m \leq o(G(R/K_1)) = [\mathbf{R}: \mathbf{K}_1] \leq [\mathbf{K}_2 : \mathbf{K}_1] = m$$

We conclude that $\mathbf{R}=\mathbf{K}_2$. □

Page 313, line 22: It is easy to see that $\mathbf{L}=\mathbf{F}(x_1, x_2, x_3)$, and the $\cdots$

page 315, line 11:

$$\Delta \mapsto \overline{\Delta} = \sqrt{-4\theta_2^3 - 27\theta_3^2}$$