

## 整数論 1 の正誤表

1. p.7, l.-7,  $x = \pm\sqrt{6+3y^2} \rightarrow x = \pm\sqrt{6+2y^2}$
2. p.20, (1.4.22) のすぐ下,  $a_i$  は  $i$  の位の数である  $\rightarrow a_i$  は  $\ell^i$  の位の数である
3. p.31. l.-2, 命題 1.4.7 (2) より  $\rightarrow$  命題 1.4.20 (2)
4. p.33, 1.8 節はじまって 7 行目,  $b=0$  の場合はやさしいので  $\rightarrow$  1 行前に「 $b$  を法として考えるので,  $b \neq 0$  である。」と入れる. 「 $a=0$  の場合はやさしいので  $a \neq 0$  と仮定する。」とする.
5. p.43, 命題 1.9.8 の証明が終わってから 3 行目,  $\phi(x)^{169} \rightarrow f(x)^{169}$
6. p.43, l.-1,  $250^2 \bmod 1081 \rightarrow 250^4 \bmod 1081$
7. p.48, 例題 1.10.8 のあと, 証明  $\rightarrow$  解答
8. p.52, l.7,  $y_1 \rightarrow y_2$  (2 箇所)
9. p.53, 命題 1.11.2 の証明 3 行目, 0 以外の平方剰余は (1.11.3) と合同である  $\rightarrow$  0 以外の平方剰余は (1.11.3) のどれかと合同である
10. p.55, l.7,  $b_j \leq (p-1)/2$  が誤り. 「しかし\*\*\*」を「 $a_i \equiv sn, b_j \equiv tn$  ( $1 \leq s, t \leq (p-1)/2$ ), なら,  $a_i + b_j \equiv 0 \bmod p$  より  $s + t \equiv 0 \bmod p$  となる. しかし,  $2 \leq s + t \leq 2 \cdot (p-1)/2 = p-1$  なので矛盾である。」とする.
11. p.60, 例 1.11.14 173  $\rightarrow$  179 (2 箇所)  
以上, Mmtheta 様ご指摘有難うございました.
12. p.82, l.2, メルセンヌ数  $\rightarrow$  メルセンヌ素数
13. p.134, 5.2.8 (2)  $G = \mathfrak{S}_3$  とする.
14. p.271, 8.8 節, 高木貞治「初等整数論講義」でも使われているイデアルの  $\mathbb{Z}$  基底の記号  $[a, b]$  だが, 2 巻でイデアルの類を  $[I]$  と書いたりするときにかぎ括弧が都合が悪く, また他にもかぎ括弧はいろいろ使っているので, 2 巻でイデアルの  $\mathbb{Z}$  基底に  $\langle a, b \rangle$  という記号を使うことにした 1 巻自身の中でこの記号で不都合になることはないが, 増刷することがあれば, この記号は 2 巻の記号に統一すると思う.  $[, ]$  を  $\langle, \rangle$  にするのは p.271, l.-3,-2, 2 箇所, 定理 8.8.1 の中 1 箇所, p.272, l.-4 2 箇所, p.273, l.8 2 箇所, 定理 8.8.4 の中 1 箇所, p.274, l.-6,-5, 5 箇所. p.271, l.-2 は「結果的\*\*\*」の文は「なお, [13] では  $\langle \alpha, \beta \rangle$  ではなく,  $[\alpha, \beta]$  という記号が使われているが, 2 巻でイデアル  $I$  の類を  $[I]$  と書くので, この記号にする。」と変更.

15. p.272, 1.5,  $|b| < \sqrt{|D|/3}$  を  $|b| \leq \sqrt{|D|/3}$  と変更. (A) の最後に「ただし,  $D \neq -3$  なら,  $|b| < \sqrt{|D|/3}$  としてよい。」と入れる. 1.10,  $[ , ]$  を  $\langle , \rangle$  とする.
16. p.344, 演習問題 7.4.1 の解答,  $\bar{\alpha}$  が原始元  $\rightarrow \bar{\alpha}$  が原始根
17. p.316, オーダーは仮定 8.3.2 を満たすものについて示したが,  $\mathbb{Z}_p$  が仮定 8.3.2 を満たすことを示す前にオーダーを使ってしまっている. だから, 次の変更を行う.

定理 9.1.26 (7) の証明の最後の部分を次のように変更.

$I \subset \mathbb{Z}_p$  を零でないイデアルとする.  $I$  の元  $x$  で  $|x|_p$  が最大のものをとる. 補題 9.1.24 より  $n \geq 0$  があり,  $|x|_p = |p^n|_p$  となる.  $|p^{-n}x| = |(p^{-n}x)^{-1}|_p = 1$  なので, (5) より  $p^{-n}x \in \mathbb{Z}_p^\times$  である. よって,  $x\mathbb{Z}_p = p^n\mathbb{Z}_p$ .  $y \in I$  なら,  $|x^{-1}y|_p \leq 1$  である. よって, (5) より  $x^{-1}y \in \mathbb{Z}_p$  である. したがって,  $y \in x\mathbb{Z}_p$  となる.  $y \in I$  は任意なので,  $I = x\mathbb{Z}_p = p^n\mathbb{Z}_p$  である. これより,  $\mathbb{Z}_p$  は単項イデアル整域で, すべての零でないイデアルは  $p^n\mathbb{Z}_p$  という形である. 特に,  $\mathbb{Z}_p$  は正規環である. よって,  $\mathbb{Z}_p$  はデデキント局所環, つまり離散付値環である.

また, 系 9.1.27 の後を次のように変更

$\mathbb{Z}_p$  が仮定 8.3.2 を満たすことはこの後命題 9.1.31 で示すが, 定理 9.1.26 (7) の証明で  $\mathbb{Z}_p$  の任意のイデアルが  $p^n\mathbb{Z}_p$  であることを示したので, 定義 8.4.3 と同様にそのオーダーを定義できる.  $a \in \mathbb{Q}$  なら,  $a = p^n c/d$  ( $c, d \in \mathbb{Z} \setminus \{0\}$  は  $p$  で割れない) とすると, 定理 9.1.26 (6) と (7) の証明より  $|c/d|_p = 1$ ,  $a\mathbb{Z}_p = p^n\mathbb{Z}_p$  である. したがって,  $a$  の  $\mathbb{Q}_p$  でのオーダーと  $\mathbb{Z}$  の極大イデアル  $p\mathbb{Z}$  による  $\mathbb{Q}$  でのオーダーは一致する. これが成り立つので,  $\mathbb{Q}_p$  におけるオーダーも  $\text{ord}_p(a)$  と書く. 定理 9.1.26 (6) より,  $|a|_p = p^{-\text{ord}_p(a)}$  となる. したがって,  $x, y \in \mathbb{Q}_p$  なら  $|x - y|_p$  は加法的付値  $\text{ord}_p$  により定まる距離である. これはまとめて命題の形に書いておく.

レイアウトの関係で p.316, 1.2 の  $x \cdot y$  をディスプレイでなくする.

18. p.266, 1.10, 持つことは  $\rightarrow$  持たないことは
19. p.274, 1.13,  $(3, -4, -3) \rightarrow (3, -4, -2)$
20. p.284, 1.17,  $x^3 + x - 2x - 1 \rightarrow x^3 + x^2 - 2x - 1$
21. p.287, 1.-3,  $(\sigma_i(\zeta^j)) \rightarrow (\sigma_j(\zeta^i))$
22. p.288, 1.-5,  $\text{ord}_i(b_i) \rightarrow \text{ord}_p(b_i)$
23. p.290, 1.2,  $(\zeta - \zeta^{i-j})y \rightarrow (1 - \zeta^{i-j})x$
24. p.290, 1.15,  $J$  がイデアルなら  $J_i^h$  は単項イデアルになる.  $\rightarrow J_i^h$  は単項イデアルになり,

25. p.291, 1.6  $u = \zeta^a u_1, \rightarrow u = \zeta^r u_1$

以上, 18-25, 大阪府立大手前高校, 深川久様ご指摘有難うございました.

26. 3巻の目次で 1.1 節が増えたのを追加する.

### 整数論 1 初版第 2 刷の正誤表

1. 命題 6.8.33 の主張で最初の  $X$  を  $X \neq \emptyset$  とする. また, 証明をつける. 証明は以下のようにする.

$X$  に極大元がないとして矛盾を導く.  $I_1 \in X$  とすると,  $I_1$  が極大元ではないので,  $I_1 \subsetneq I_2$  となる  $I_2 \in X$  がある. これを繰り返せば, イデアルの無限に続く増加列  $I_1 \subsetneq I_2 \subsetneq \dots$  が得られ, 矛盾である.

2. 定理 6.8.38 の証明

p.190, 1.-6, 「\*\*\*  $(a_1)$  が極大であるものをとる (命題 6.8.33 の  $X$  として, 生成系  $\{x_1, \dots, x_n\}$  の関係式の最初の係数で生成されるイデアル全体の集合をとる). とする.」

3. p.191, 1.1, 「 $i = 2$  としてよい.」の後を次のようにする. 「 $x_1, \dots, x_n, a_1, \dots, a_n$  の代わりに  $x_2, x_1, \dots, x_n, a_2, a_1, \dots, a_n$  を考えると, これに対応する「 $a_1$ 」というのは関係式の係数の最初の元なので,  $a_2$  である.  $(a_1) \subsetneq (a_2)$  なので,  $a_1$  のとりかたに矛盾する. したがって,  $(a_1) = A$ , つまり  $a_1 \in A^\times$  である.」

これで不必要な数行を削除できる.

4. 補題 7.1.10 の証明.  $x \in L$  とする.  $\{1, x, x^2, \dots\}$  が無限集合なら,  $n > 0$  があり,  $\{1, \dots, x^n\}$  は 1 次従属である. \*\*\*\*  $\{1, x, x^2, \dots\}$  が有限集合なら,  $0 \leq n < m$  があり,  $x^n = x^m$  となる.  $x = 0$  なら,  $x$  は明らかに  $K$  上代数的である.  $x \neq 0$  なら,  $x^n(1 - x^{m-n}) = 0$  より  $x^{m-n} = 1$  である. よって, この場合も  $x$  は  $K$  上代数的である.

5. 系 7.1.21, できれば, 主張の最後に「よって,  $\{\alpha \in L \mid \alpha \text{ は } K \text{ 上代数的}\}$  は  $L/K$  の中間体である.」と入れる.

6. 索引で「高木貞治 (1875-1960)」とする.

7. 以下 13 まで, 山口県立小野田高等学校教諭 上田政明様ご指摘どうも有難うございました.

p.217, 1.7, 式の右边を

$$p^{n(\ell-1)} + p^{n(\ell-2)} + \dots + 1$$

とする.

8. p.240, 1.-1,  $K$  における  $\rightarrow L$  における

9. p.248, 1.-7,  $JM = M$  を  $((J + I)/I)M = M$  と変更し, その後を  $J + I \subset \mathfrak{p}_i$  が\*\*\*成り立つ.  $A/I$  の極大イデアルは  $\mathfrak{p}_1/I, \dots, \mathfrak{p}_n/I$  なので,」と変更する.
10. p.250, 1.7,  $A_{\mathfrak{m}}M$  は  $L$  の部分  $A_{\mathfrak{m}}$  加群である.  $\rightarrow A_{\mathfrak{m}}M$  は  $L$  の部分  $A_{\mathfrak{m}}$  加群, よって  $L$  の部分  $A$  加群である.
11. p.250, 1.-4,  $(b_i a_i)^{-1} a_i \in \mathfrak{m}$  である.  $\rightarrow b_i a_i$  が単元で  $a_i \in \mathfrak{m}$  なので,  $(b_i a_i)^{-1} a_i \in \mathfrak{m}$  である.
12. p.316, 1.6,  $x \in \mathbb{Q}_p \setminus \{0\} \rightarrow x \in \mathbb{Q}_p$
13. p.329, 1.-8, 一番右の  $-1$  は  $1$  にする. 1.-4,  $1 \cdot (-1) \cdot (-1) \cdot (-1) = -1$ .  $\rightarrow 1 \cdot (-1) \cdot (-1) \cdot 1 = 1$ .
14. 命題 1.4.12 で  $ab/\ell$  が整数であることが証明されていない. だから 命題 1.4.12 と系 1.4.13 を系 1.5.7 の後に移動して, 証明の途中の「一方」の後に「 $ab$  は  $a, b$  の公倍数なので, 系 1.5.7 より  $ab/\ell \in \mathbb{Z}$  である.」と入れる.  
また, 系 1.5.7 の後半部分の証明を以下のように変更する.  
 $\ell = \text{lcm}(a, b)$  で  $n$  を  $a, b$  の公倍数とする.  $-1$  倍することにより  $n > 0$  と仮定してよい.  $n$  を  $\ell$  で割り算し,  $n = q\ell + m, q, m \in \mathbb{Z}, 0 \leq m < \ell$  とする.  $n, \ell$  は  $a, b$  の公倍数なので,  $m = n - q\ell$  も  $a, b$  の公倍数である. もし  $m > 0$  なら,  $\ell$  が  $a, b$  の最少公倍数であることに矛盾する. したがって,  $m = 0$  であり,  $n$  は  $\ell$  の倍数である.  
また, 1.4, 1.5 節の命題や定理の番号が変わるので, 引用されている番号を変える.  
木下通宏様ご指摘有難うございました.
15. 以下 34 まで山口県立小野田高等学校教諭 上田政明様ご指摘どうも有難うございました.  
p.165, 1.9, 「写像  $S^{-1}A \rightarrow K$  が定まる \*\*\* 単射である.」を以下のように変更する. 「命題 6.5.5 より, 写像  $S^{-1}A \rightarrow K$  が定まる.  $a \in A, s \in S$  で  $a/s$  が  $K$  で  $0$  なら,  $K$  において  $a = s(a/s) = 0$  である.  $A \subset K$  なので,  $a = 0$ , よって  $S^{-1}A$  においても  $a/s = 0$  である. よって,  $S^{-1}A \rightarrow K$  は単射である.」
16. p.177, 命題 6.7.2 (1)  ${}^t(A + B)$  とする.
17. p.183, 例 6.8.18,  $\text{Coker}(\pi) = \{0\}$ .
18. p.194, 6.8.2,  $R^4 \rightarrow R^2$
19. p.194, 6.8.4,  $T_1, T_2$  の前に 「 $B = PAQ,$ 」 と入れる.
20. 7.1 節の最初, 「 $Z \ni n \mapsto n \cdot 1 \in K,$ 」 「 $\text{Im}(\phi)$  は  $K$  の部分環」

21. p.211, l.1,  $\overline{M_{i-1}}$  を  $\overline{\psi(M_{i-1})}$  とする. p.217, 定理 7.4.10 の証明の 1 行目, 「 $G$  が巡回群であること\*\*\*」の文を削除 (帰納法を使っていない).
22. p.221, l.5, 「である。」の後を「 $\tau \in H$  のとき,  $\{\tau\sigma \mid \sigma \in H\} = H$ 」と変更する.
23. p.240, 命題 8.1.24 の証明の 1 行目,  $\{x_1, \dots, x_n\} \subset B$  とする.
24. p.248, l.14,  $0_K \rightarrow \mathcal{O}_K$
25. p.255,256, 補題 8.3.23 の主張で  $a_1, \dots, a_t \in \mathbb{Z}$  の部分を  $a_1, \dots, a_t \geq 0$  と変更する. また, 証明を次のように変更する.  
(最初の (1) は削除して)  $t = 2$  なら,  $\mathfrak{p}_1^{a_1} = \mathfrak{p}_1^{a_1} \cdot \mathfrak{p}_2^0$ ,  $\mathfrak{p}_2^{a_2} = \mathfrak{p}_1^0 \cdot \mathfrak{p}_2^{a_2}$  なので, 定理 8.3.17 (3) より,  

$$\mathfrak{p}_1^{a_1} \cap \mathfrak{p}_2^{a_2} = \mathfrak{p}_1^{\max\{a_1, 0\}} \mathfrak{p}_2^{\max\{0, a_2\}} = \mathfrak{p}_1^{a_1} \mathfrak{p}_2^{a_2}$$
である. 一般の場合はこのような考察を繰り返せばよい.  
なお, 補題の主張は中国剰余定理からも従う.  
命題 8.3.24 は (2) の部分の証明を次のように追加する.  
(2)  $I_1 \subset I_2 \subset K$  が分数イデアルなら,  $I_2 = Aa_1 + \dots + Aa_n$  とすると,  $c \in A \setminus \{0\}$  があり,  $ca_1, \dots, ca_n \in A$  となる. すると,  $cI_1 \subset cI_2 \subset A$  である. 定理 8.3.17 (2) より, イデアル  $J \subset A$  があり,  $cI_1 = cI_2J$  である. すると,  $I_1 = I_2J$  である.  
定理 8.3.17 の主張 (3) に対応する部分も (1), (2) のように,  $A$  の元を分数イデアルにかけて,  $A$  のイデアルの場合に帰着すればよい. 詳細は省略する.
26. p.251, 系 8.3.16 で「 $A$  の分数イデアル」を「 $K$  の分数イデアル」とする.
27. p.278, l.17,  $y^2 = -2NN_{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}(\alpha)$  を  $y^2 = 2NN_{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}(\alpha)$  とする.
28. p.279, l.-1, 違いではないが,  $y^2 + 5 \equiv 6 \pmod{8}$ ,  $x^3 \equiv 0 \pmod{8}$  を  $y^2 + 5 \equiv 2 \pmod{4}$ ,  $x^3 \equiv 0 \pmod{4}$  とする.
29. p.290, l.-7,-5, 対称式  $\rightarrow$  基本対称式 とする (なお, 変数の個数が限られているので, 基本対称式の数は有限個です).
30. p.292, l.-1,  $y \equiv 0 \pmod{p\mathbb{Z}[\zeta]}$  を  $y \equiv 0 \pmod{p\mathbb{Z}}$  とする. その文の後に p.293 の最初の行は「これは矛盾である。」とする.
31. p.281, 定義 8.11.1,  $i < n$  を  $0 < i < n$  とする.
32. p.314, l.11, 「 $z_1 \in \mathbb{Z}$  がある。」の後, 「 $z_1$  を  $p$  で割った余りを考え  $0 \leq z_1 < p$  としてよい。」と入れる. l.13 では 「 $z_2 \in \mathbb{Z}$  で  $0 \leq z_2 < p$  となるものがある。」とする.

33. p.317, 1.6, 間違いではないが, 「距離である。」の後, 「補題 9.1.25 より  $\mathbb{Q}$  は  $\mathbb{Q}_p$  で稠密なので,  $|x - y|_p$  で定まる距離により  $\mathbb{Q}_p$  は  $\mathbb{Q}$  の完備化となる。」と入れる.
34. p.318, 1.-3, 間違いではないが, 定理 9.1.2  $\rightarrow$  定理 9.1.2 と命題 6.5.8
35. 命題 5.2.41, 証明の第一段落の終わりに, 「 $N$  は  $G$  の正規部分群なので,  $HN$  の部分群でもある。」と入れる.
36. 命題 5.2.43 の証明の第 4 行, 「 $y \in N$ 」は削除.
37. p.334, 1.4.6, 「 $2^k$  を  $n$  以下の最大の 2 べきとすると,  $n$  以下の整数で  $2^k$  で割り切れるものは  $2^k$  だけであることを証明せよ。」として以前あった文は削除. このヒントのほうがより親切. こういう方針も本当は自分で考えるほうがよいのだが。
38. p.119, 1.2,  $\text{Ker}(\phi) = \{1_G\}$  を  $\text{Ker}(\phi) = \{(1_G, 1_G)\}$  と変更.
39. p.151, 1.8,  $q_1(x) = q_2(x) = 0$  の  $= 0$  を削除.
40. 命題 5.2.20 (1)  $C$  を  $H$  と変更.
41. p.113, 1.3,  $G/H, H \setminus G$  を  $G/H (H \setminus G)$  と変更.
42. 注 5.3.8 の 5 行目,  $k \in G \setminus H$  なら,  $(k, 1H) \mapsto kH \neq 1H$  である. よって, \*\*\* と変更する.

### 整数論 1 初版第 3 刷の正誤表

1. p.319, 1.-4,  $x_i \in \mathbb{Z}$  を  $x_i \in \mathbb{Z}_p$  と変更.
2. 定義 6.8.5, 左加群  $\rightarrow$  加群
3. 次の 3-35 については井上亜星様, ご指摘有難うございました. p.84, 1.10, 「 $m$  の個数は  $n$  なので」を「 $m$  の個数は  $n - 1$  で  $d = n$  なら  $\phi(n/d) = 1$  なので」と変更する.
4. p.126, 1.8, 「 $(k, 1H) \rightarrow kH$  であり,  $k \notin H$  である  $k \in G$  があるので,  $\phi$  は自明な準同型ではない。」とする (推移的という用語をまだ定義していないので).
5. 命題 6.8.26 の証明の 2 行目,  $=$  を  $\rightarrow$  に変更.
6. p.199, 1.13, 間違いではないが「零でない  $f(\alpha) = 0$  となる多項式で次数が最小なもの」とする.
7. p.205, 命題 7.1.26, 証明の 4 行目, 「命題 6.1.27 より  $\Phi$  は単射」を「系 6.1.28 より  $\Phi$  は単射」と変更.

8. p.208, 1.2, 「 $f(\alpha) = 0$  なら, 次の (1), (2) は同値である。」とする.
9. p.210, 1.-5, 「 $\xi \in ***$  の元に」を「 $\xi \in ***$  に」と変更.
10. p.211, 1.-3, 7.1.26 より \*\*\* 1.-2 の延長することができる. 7.2.7 より,  $\phi \in \text{Hom}_K^{\text{al}}(L, \overline{K})$  で  $\phi(\alpha) = \beta$  となる.
11. p.221, 1.7-9,  $H_M$  を  $H(M)$  と変更.
12. p.197, 間違いではないが,  $M_1 \cdot M_2$  を記号索引に入れる.
13. p.221, 1.-9, 命題 7.4.3(2)  $\rightarrow$  定理 7.3.9
14. p.344, 7.4.1 (4) の答え  $\overline{20}$  は  $\overline{10}$  に変更. 場所も変える.
15. p.346, 1.5, 7, 9, 11  $15 - 3\sqrt{5}$  を  $15 + 5\sqrt{5}$  と変更.  $-3/20$  を  $1/4$  と変更.  $-9/400$  を  $5/64$  と変更.  $c^2 = 3/8 \pm 1/4 = 5/8, 1/2$  と変更.
16. p.241, 1.7 「もし  $\{x_1, \dots, x_m\}$  が 1 次従属なら,」を削除し, 1.8 の 「となる。」を「とする。」とする.
17. p.242, 1.10,  $a_0 a_1 (a_0 x)^{n-1}$  を  $a_1 (a_0 x)^{n-1}$  と変更.
18. 間違いではないが, p.148 の  $\mathbb{F}_p$  と p.216 の  $\mathbb{F}_q$  を索引に入れる.
19. p.257, 定義 8.4.3 の 5 行目,  $\mathbb{Q}$  のオーダー  $\rightarrow a \in \mathbb{Q}$  のオーダー
20. p.271, 1.-4, 計算法に述べる  $\rightarrow$  計算法を述べる
21. p.351, 問 8.8.1 (3) の答え,  $(a, b, c) = (1, 1, 3)$  が正しい.
22. p.352, 問 8.8.2 (1) の答え,  $(a, b, c) = (1, -2, -1)$
23. p.352, 問 8.8.2 (2) の答え,  $(a, b, c) = (1, -2, -2), (2, -2, -1)$ . 対応する無理数  
が同じ循環節を持つので, 類数は 1.
24. p.353, 問 8.8.2 (8) の答え,  $(a, b, c) = (5, -2, -5)$  が抜けている.
25. p.353, 問 8.9.1(2) の答え,  $\text{mod } 7$  を  $\text{mod } 28$  と変更.
26. p.353, 問 8.9.1(5) の答え,  $p \equiv 1 \pmod{4}$  なら, \*\*\*  $p \equiv 1, 73, 9, 85, 45, 13, 49, 41, 81, 77, 29$   
 $\pmod{92}$  の 45 を 25 に変更.  
  
 $p \equiv 3 \pmod{4}$  なら, \*\*\*  $p \equiv 2, 5, 7, 10, 11, 14, 15, 17, 19, 20, 21 \pmod{23}$  の 2  
を削除し, 21 の後に 22 を入れる.  
  
 $p \equiv 71, 51, 7, 79, 11, 83, 15, 63, 19, 43, 67 \pmod{92}$  の 71 を削除し, 最後に 91 を  
追加.

27. p.354, 問 8.9.2(2) の答え, 「 $p \equiv 1, 4, 9, 16, 8, 2, 15, 13 \pmod{17}$ 」とする (13 が抜けている).
28. p.354, 問 8.9.2(3) の答え,  $p = 3, 7$  または \*\*\* とする.
29. p.354, l.-1,  $(19/p) = 1$  を  $(-19/p) = 1$  と変更.
30. p.355, 問 8.9.3 の答え, (1)  $p = 7$  または, \*\*\* とする. (2)  $p = 11$  または, \*\*\* とする.
31. p.302, 8.11.2  $\cos 2\pi/n$  を  $2 \cos 2\pi/n$  と変更.
32. p.280, l.-9,  $n > 1$  を  $n > 0$  と変更.
33. p.281, l.1,  $n > 1$  を  $n > 0$  と変更.
34. p.281, 定義 8.11.1, 最後に「なお  $\Phi_1(x) = x - 1$  である。」と追加.
35. p.322, 命題 9.2.2 (2) の証明の最後に「 $x = y = 1$  なら  $ax^2 + (1-a)y^2 = 1$  なので,  $(a, 1-a) = 1$  である。」と追加.
36. p.332, 問 9.1.4 の 1 行目,  $(a, b) \in \mathbb{Z}$  を  $a, b \in \mathbb{Z}$  と変更.
37. p.95, l.10,

$$1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{\theta}}} = 1 + \frac{1}{2 + \frac{\theta}{3\theta + 1}} = 1 + \frac{3\theta + 1}{7\theta + 2} = \frac{10\theta + 3}{7\theta + 2}$$

と変更.

以下の 38-48 はハンドルネーム「ほら」氏による.

38. 演習問題 6.6.3, 「 $\phi: A[x, y] \rightarrow A[t]$  を  $\phi(x) = at, \phi(y) = bt$  である  $A$  準同型とするととき」と訂正
39. 定義 6.8.5 左加群  $\rightarrow$  加群 (既出だった)
40. p107 l.6, 有限群  $\rightarrow$  群
41. p.136, l.9,  $x_2, x_3, x_4$  を  $x_1, x_2, x_3$  と変更.
42. p.142, l.13, 定義 6.1.16 から命題 6.1.17 の証明の終わりまで, 例 6.1.23 の後に移動.
43. p.146, l.4,  $B$  を  $\text{Im}(\phi)$  と変更.

44. p.150, 命題 6.2.13,  $A$  を整域  $\rightarrow A$  を環. 証明で 命題 6.2.10 (3) より\*\*\* の部分を「命題 6.2.10 (2) より,  $q_1(x) - q_2(x) \neq 0$  なら, 左辺の次数は  $\deg f(x)$  以上となり矛盾である.」と変更.
45. p.182, 定義 6.8.2 の後のコメントを 定義 6.8.3 の後に移動.
46. p.183, 1.22,  $\text{Coker}(\pi) = \{0\}$ .
47. p.192, 6.2.5  $B$  の定義で  $2i + 3j \geq 0$  を削除.
48. p.193, 6.6.4 (2) (3)  $\rightarrow$  イデアル (3)
49. p.110, 1.11,  $x_1^\pm \cdots x_t^\pm$  を  $x_1^{\pm 1} \cdots x_t^{\pm 1}$  に変更.

#### 整数論 1 初版第 4 刷の正誤表

1. p.261, 1.3,  $K = \mathbb{Q}$  を  $A = \mathbb{Z}$  と変更.
2. 2-8 については杉山真吾さん有難うございました. p.219, 1.7,  $K(\alpha_1, \dots, \alpha_{n-2}, \alpha)$  を  $K(a_1, \dots, a_{n-2}, \alpha)$  と変更.
3. p.219, 1.15,16,  $\phi_i(\alpha_1) = \phi_i(\alpha_2), L = K(\alpha_1, \alpha_2)$  の  $\alpha_1, \alpha_2$  は  $a_1, a_2$ .
4. p.241, 系 8.1.25 (3), 「素イデアル  $P$  があり\*\*\*」と変更する.
5. p.344, 7.3.1 (2) の解説の最後に「なお  $\sqrt{(1 + \sqrt{-3})/2} = (\sqrt{3} + \sqrt{-1})/2$  である.」と入れる.
6. p.225, 7.4.6 (3)  $\tau$  を  $\sigma$  と変更 (2箇所).
7. p.346, 7.4.8 (4) の解説, 1.5, 最後は  $(15 - 3\sqrt{5})/20$  ではなく  $(3 + \sqrt{5})/4$ . p.7 の最後も同じ. 1.9, 最後は  $2cd = 1/4$ . 1.11,

$$c^4 - \frac{3}{4}c^2 + \frac{5}{64} = 0.$$

1.13,

$$c^2 = \frac{3}{8} \pm \frac{1}{4} = \frac{5}{8}, \frac{1}{8}$$

1.15,16, 「なお\*\*\*導ける.」を削除.

8. p.346, 1.-8,  $a, b \in \sqrt{2}$  を  $a, b \in \mathbb{Q}(\sqrt{2})$  と変更.
9. p.46, 1.-6, 命題 1.4.18 (2)  $\rightarrow$  命題 1.4.18 (1) p.191,  $(a_1) \subsetneq (a_2)$  の部分は「 $(d) = (a_1, a_2)$  とする. このとき,  $a_1s + a_2t = d, a_1 = db_1, a_2 = db_2$  となる  $s, t, b_1, b_2 \in A$  があり,  $b_1s + b_2t = 1$  となる.  $y_1 = b_1x_1 + b_2x_2, y_2 = tx_1 - sx_2$  とおくと,  $x_1 = sy_1 + b_2y_2, x_2 = ty_1 - b_1y_2$  であるので,  $M$  は  $y_1, y_2, x_3, \dots, x_n$  で生成さ

れる. また,  $dy_1 + a_3x_3 + \cdots + a_nx_n = a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n = 0$  である. 以上から,  $x_1, x_2, x_3, \cdots, x_n$  を  $y_1, y_2, x_3, \cdots, x_n$  に,  $a_1, a_2, a_3, \cdots, a_n$  を  $d, 0, a_3, \cdots, a_n$  に取りかえても条件はみたされるが,  $(a_1) \subsetneq (d)$  であり  $(a_1)$  の極大性に反する.」 とする  $a_1, a_2$  を入れ替える部分は削除.

10. 補題 9.1.24 の証明で「したがって  $|x|_p = C$  である.」を削除.

### 整数論 1 初版第 6 刷の正誤表

1. p.262, l.5,  $d \equiv 1, 2 \pmod{4}$  なら,  $-d \equiv 2, 3 \pmod{4}$  なので
2. p.310, l.-4 から p.311, l.15 までは以下のように変更. 上智大の角皆様 (あるいはその学生さん) ご指摘有難うございました. このような初歩的な間違いを 10 年間放置してとても恥ずかしい.

次に  $(\hat{X}, \hat{d})$  が完備であることを示す.  $x_m = \{x_{m,n}\}_n \in \hat{X}$  とし,  $\{x_m\}_m$  がコーシー列であるとする. 各  $m \geq 0$  に対し  $N_m > 0$  を  $m_1 < m_2$  なら  $N_{m_1} < N_{m_2}$  であり,  $l_1, l_2 > N_m$  なら  $d(x_{m,l_1}, x_{m,l_2}) < 1/m$  となるように選ぶ.  $X$  の列  $\tilde{x}$  を  $\tilde{x} = \{x_{m,N_m+1}\}_m$  と定める.  $\tilde{x}$  が  $X$  のコーシー列で

$$(1) \quad \lim_{m \rightarrow \infty} x_m = \tilde{x}$$

となることを示す.

$\epsilon > 0$  とする.  $\{x_m\}$  がコーシー列なので, 整数  $M_1(\epsilon) > 1/\epsilon$  があり,  $m_1, m_2 > M_1(\epsilon)$  なら  $\hat{d}(x_{m_1}, x_{m_2}) < \epsilon$  となる.  $l$  を十分大きく取ると,  $d(x_{m_1,l}, x_{m_2,l}) < 2\epsilon$  となる. すると

$$\begin{aligned} d(x_{m_1, N_{m_1}+1}, x_{m_2, N_{m_2}+1}) &\leq d(x_{m_1, N_{m_1}+1}, x_{m_1, l}) + d(x_{m_1, l}, x_{m_2, l}) \\ &\quad + d(x_{m_2, l}, x_{m_2, N_{m_2}+1}) \\ &< \frac{1}{m_1} + 2\epsilon + \frac{1}{m_2} < \frac{2}{M_1(\epsilon)} + 2\epsilon < 4\epsilon \end{aligned}$$

となるが, 得られた不等式は  $l$  に依らないので,  $\tilde{x}$  はコーシー列である.

(1) を示す.  $\epsilon > 0$  に対し  $M_1(\epsilon)$  を上のように選び,  $m > M_1(\epsilon)$  とする. 定義より  $\hat{d}(x_m, \tilde{x}) = \lim_{l \rightarrow \infty} d(x_{m,l}, x_{l, N_l+1})$  である.  $l > m, N_m$  が十分大きければ,  $|\hat{d}(x_m, \tilde{x}) - d(x_{m,l}, x_{l, N_l+1})| < \epsilon$  である.  $l > m > M_1(\epsilon)$  なので, 上と同様に,  $l_1 > N_m, N_l$  がさらに大きければ,  $d(x_{m,l_1}, x_{l,l_1}) < 2\epsilon$  となる.  $l > m > M_1(\epsilon)$  なので,

$$\begin{aligned} d(x_{m,l}, x_{l, N_l+1}) &\leq d(x_{m,l}, x_{m, l_1}) + d(x_{m, l_1}, x_{l, l_1}) + d(x_{l, l_1}, x_{l, N_l+1}) \\ &< \frac{1}{m} + 2\epsilon + \frac{1}{l} < 4\epsilon. \end{aligned}$$

これより  $d(x_m, \tilde{x}) < 5\epsilon$ . したがって, (1) が成り立ち,  $(\hat{X}, \hat{d})$  は完備である.

3. p.228, 命題 8.1.3 は「代数学 2」 p.138, 命題 2.8.2 により変更する.

#### 整数論 1 初版第 7 刷の正誤表

1. p.175, 1.-6-1.-3,  $g_1(x)$  などを  $h_1(x)$  などに変更.

2. p.287, 1.-5, 「証明を続ける。」の後に追加,

$\mathcal{O}$  を  $\mathbb{Q}(\zeta)$  の整数環とすると,  $\mathcal{O}$  は  $\mathbb{Z}[\zeta]$  上整である.  $P$  を  $(1 - \zeta) \subset \mathbb{Z}[\zeta]$  上の素イデアルとし,  $v(x) = \text{ord}_P(x)$  を  $P$  により定まる  $\mathbb{Q}(\zeta)$  のオーダーとする (定義 8.4.3 参照). また  $\text{ord}_p(\cdot)$  を  $p$  により定まる  $\mathbb{Q}$  上のオーダーとする.  $v(1 - \zeta) = a$  とすると,  $v(p) = a(p - 1)$  である (定理 II-1.3.23 より  $a = 1$  となる).

p.288, 1.7-9, 「 $v(x) \geq 0$ 」より前を削除.

p.288, 1.-10, 1.-7, 右辺を  $a$  倍にする. 1.-10 では  $a((p - 1)\text{ord}_p(b_i) + i)$ .