「素数と 2 次体の整数論」(青木昇著) 初版第 1 刷正誤表 (2016.12.15)

頁	行	誤	正
vi	下から 9 行目	桑田泰孝	桑田孝泰
2	7 行目	$\alpha = a + bi, \ = c + di$	$\alpha = a + bi, \ \beta = c + di$
〃	下から 6 行目	加法と乗法	加法, 減法および乗法
〃	脚注	Zahlen	Zahl
5	定義 1.4 の 1 行目と 2 行目	$a_1, \ldots, a_r$	$a_1, \ldots, a_n$
7	1 行目	$ax + (bc)y = 1$	系 1.7 より $ax + (bc)y = 1$
〃	下から 7 行目	整数 a に対し,	整数 a に対し, 集合
11	定理 1.18 [証明] の 2 行目	$i = 1, \ldots, r$	$i = 1, \ldots, n$
14	系 1.24 の 1 行目	任意の整数	整数
17	2 行目と 3 行目	p_s	p_r
〃	6 行目	$p = p_i(\exists i)$	$p = p_i \ \ (\exists i \in \{1, \ldots, r\})$
〃	7 行目	$p \neq p_i(\forall i)$	$p \neq p_i \ \ (\forall i \in \{1, \ldots, r\})$
〃	命題 1.27 の 1 行目	$v_p(v)$	$v_p(b)$
18	6 行目と問題 1.28	系 1.24	定理 1.26
19	下から 2 行目	$v_p(\mathrm{GCD}(a, b))$	$v_p(\mathrm{GCD}(a_1, \ldots, a_r))$
42	問題 2.16 の 1 行目	$0 \leq k \leq p^e$	$1 \leq k \leq p^e$
43	$\varphi(m)$ の表, $m = 10$ での値	8	4
53	13 行目	$0 \leq a < d$	$0 \leq i < d$
54	定理 2.34 [証明] の 1 行目	命題 2.33 より	このとき, 命題 2.33 より
56	例 2.38 の 1 行目	次のように	次の頁の表のように
58	下から 2 行目	わかる	判る
64	下から 3 行目	$1 \leq v_p(a) \leq e$ ならば	$1 + v_p(2) \leq v_p(a) \leq e$
65	3 行目	$> i$	$> i + t$
〃	4 行目	$v_p(k) < k$	$v_p(k) < k - 1 + v_p(2)$
68	定義 3.1 の 1 行目	奇素数 p で割れない	奇素数 p で割り切れない
71	1 行目	命題 3.5	命題 3.4
〃	2 行目	$\left(\frac{a}{p}\right) = \left(\frac{g}{p}\right)^i = (-1)^i$	$\left(\frac{a}{p}\right) = (-1)^i$
〃	3 行目	命題 3.4 より	$g^{(p-1)/2} \equiv -1 \pmod{p}$ なので (定理 2.54 の証明を参照)
72	下から 4 行目の $\left(\frac{6}{23}\right)$ の計算	$\left(\frac{3}{237}\right)$	$\left(\frac{3}{23}\right)$
73	5 行目	定理 3.15	定理 3.9
76	下から 4 行目	$q_1^* \cdots q_r^*$	$q_1^* \cdots q_s^*$
77	下から 2 行目	$\sqrt{m}$ の定義を思い出そう	$\sqrt{m}$ を次で定義する
81	問題 3.23 の 1 行目	$\zeta = \zeta_8$ とおくとき	$\zeta = \zeta_8, \ G_8 = \{1, 3, 5, 7\}$ とおくとき
82	1 行目	$\sum_{r=0}^{p-1}$	$\sum_{r=0}^{p}$
〃	2 行目	z^{-p}	ζ^{-p}
83	証明の 3 行目	従って，オイラー基準より	よって，オイラー基準より
98	5 行目	$N(\alpha) = a^2 + mb^2$	$N(\alpha) = a^2 - mb^2$

頁	行	誤	正
108	下から 3 行目	例 6.28	定理 6.27
111	補題 4.47 の 1 行目	$\mathbb{Z}[P]$	$\mathbb{Z}[\rho]$
114	4 行目と 10 行目	2ω	$\lvert\omega-\omega'\rvert$
〃	5 行目〜8 行目	$\lvert\alpha_1'\rvert = \lvert a_1+b_1\omega\rvert$ $= \lvert a_1-b_1\omega+b_1\omega+2b_1\omega\rvert$ $\le \lvert a_1-b_1\omega\rvert + \lvert 2b_1\omega\rvert$ $= \frac{1}{n_1}+2n_1\omega$	$\lvert\alpha_1'\rvert = \lvert a_1-b_1\omega'\rvert$ $= \lvert a_1-b_1\omega+b_1\omega-b_1\omega'\rvert$ $\le \lvert a_1-b_1\omega\rvert + b_1\lvert\omega-\omega'\rvert$ $= \frac{1}{n_1}+2n_1\omega$
〃	下から 8 行目	α_2	$\alpha_2 := a_2-b_2\omega$
115	下から 4 行目	$\omega-\omega'=\sqrt{d}$ であることを使い	$d=\lvert\omega-\omega'\rvert^2>0$ とおき
〃	下から 2 行目	$-\frac{1}{\sqrt{d}}<x<\ \ldots\ <y<\frac{\varepsilon_1-1}{\sqrt{d}}$	$-1<x<\ \ldots\ <y<\frac{\varepsilon_1+1}{\sqrt{d}}$
118	8 行目	漸化式と初期条件 (4.19) により数列は	フィボナッチ数列は (4.19) により
126	下から 2 行目	$2+i$	$\alpha := 2+i$
129	命題 5.15 (1) の証明	A (3 箇所)	$(\alpha_1,\ldots,\alpha_n)$
130	例 5.17 の 1 行目	イデアル有理整数	有理整数
〃	例 5.17 の次の段落 1 行目	原始イデアル	原始的イデアル
131	10 行目	$f(\xi)$	$f(\beta)$
〃	下から 2 行目	$b+w$	$b+\omega$ (w を ω に代える)
132	6 行目	$b+w$	$b+\omega$ (w を ω に代える)
135	下から 1 行目と 3 行目	ユークリッド整数環	ユークリッド整域
138	6 行目	$N(\alpha)$	$N(\delta)$
139	定理 5.33 の 5 行目	$\lvert N(\rho_1)$	$\lvert N(\rho_1)\rvert$
140	3 行目	命題	補題
〃	例題 5.35 の解答 4 行目	$1+\sqrt{-2}$	$3-2\sqrt{-2}$
145	補題 5.41 [証明] の 3 行目	p は素数	p は $\mathcal{O}_K$ の素数
146	定理 5.45 の 3 行目	π は素数	π は $\mathcal{O}_K$ の素数
〃	下から 9 行目	([証明] の 1 行目に右の文を追加)	$K=\mathbb{Q}(\sqrt{m})$ (m は平方因子を含まない整数) とする.
147	1 行目	p は素数	p は $\mathcal{O}_K$ の素数
〃	5 行目	素数がある	素数 π,π' がある
〃	12 行目	素数	$\mathcal{O}_K$ の素数
〃	下から 8 行目	a^2+mb^2	a^2-mb^2
〃	下から 7 行目	$1+5\equiv 0 \pmod 8$	$1-5\not\equiv 0 \pmod 8$
〃	下から 5 行目	$a_1^2+mb_1^2$	$a_1^2-mb_1^2$
〃	下から 4 行目	$a_1^2+5b_1^2$	$a_1^2-5b_1^2$
148	1 行目と 7 行目	素数	$\mathcal{O}_K$ の素数
150	定理 5.48 の 2 行目	素数 p	有理素数 p
〃	定理 5.48 (1)(3)	π は素数	π は $\mathcal{O}_K$ の素数
151	注意 5.49 の 5 行目	$\chi_d(p)$	$\chi_d(p_n)$
164	定義 6.4	集合 $X(A,B)$ のすべての元で生成される	集合 $X(A,B)$ を含む最小の
166	2 行目	整数により生成される	整数を含む最小の

頁	行	誤	正
168	命題 6.15 [証明] の 4 行目	これらの最大公約数を n とすると,	n を $AA' \cap \mathbb{Z} = n\mathbb{Z}$ となる自然数とすると, (定理 5.18 の上の注意を参照)
178	命題 6.35 [証明] の 4 行目	命題 6.21	命題 6.18 と命題 6.24
182	7 行目	PQ'	PQ
184	1 行目	(追加)	[証明]
〃	下から 1 行目	([証明] の 1 行目に右の文を追加)	$K = \mathbb{Q}(\sqrt{m})$ (m は平方因子を含まない整数) とする.
185	2 行目	このとき,	$m \equiv 2, 3 \pmod 4$ のとき,
〃	8 行目	(8 行目の後に右の文を挿入)	$m \equiv 1 \pmod 4$ のときは, $a^2 \equiv m \pmod p$ をみたす奇数 a を取り, $P = [p, \frac{a+\sqrt{m}}{2}]$ とおいて上と同様の議論を繰り返せばよい.
〃	10 行目	$N(\omega) = 2n$	$N(\omega) = -2n$
〃	下から 3 行目	$P = [p, \sqrt{m}]$ とおけば,	$m \equiv 2, 3 \pmod 4$ のときは $P = [p, \sqrt{m}]$ とおき, $m \equiv 1 \pmod 4$ のときは $P = [p, \frac{p+\sqrt{m}}{2}]$ とおけば,
193	下から 6 行目	$\mathcal{C}_K$	$\mathcal{J}_K/\mathcal{P}_K$
195	定理 7.8 [証明] の 5 行目	$P_i \longrightarrow p_i$	$p_1, \ldots, p_r$
〃	定理 7.8 [証明] の 7 行目	$A = P_1 P_1' \cdots P_r P_r'$ である.	A の素イデアル分解に現れる素イデアルは $P_1, P_1', \ldots, P_r, P_r'$ に含まれる.
199	9 行目	$f(n-1)$	$f(q-1)$
201	下から 1 行目	64	58
202	例 7.18 (2) の 2 行目	$y^2 = x^3 - 1$	$y^2 = x^3 - 2$
207	定理 7.23 [証明] の 5 行目	$(\exists a, b)$	$(\exists a, b \in \mathbb{Z})$
209	1 行目	([証明] の 1 行目に右の文を追加)	$K = \mathbb{Q}(\sqrt{m})$ とする.
〃	10 行目	単項イデアルイデアル	単項イデアル
211	注意 7.29 の 5 行目	$N(\epsilon) = 1$	$N(\epsilon) = -1$
〃	注意 7.29 の 6 行目	$N(\epsilon) = -1$	$N(\epsilon) = 1$
223	問題 1.28 の解答	(全文を右のように変える.)	$ab = \pm \prod_p p^{v_p(ab)}$ と $ab = \pm \prod_p p^{v_p(a)+v_p(b)}$ において, 各 p の指数が等しいこと.
〃	下から 1 行目	$e > f$	$e < f$
224	問題 1.32 (2) の解答	m, n	m, n をすべて b, c に変える.
〃	下から 7 行目	$v_p(x) \geq 0$ かつ $v_p(y)$.	$v_p(x) \geq 0$ かつ $v_p(y) \geq 0$.
225	問題 1.50 の解答	$\mathrm{GCD}(m, 2m) = 1$	$\mathrm{GCD}(m, 2n) = 1$
226	問題 3.3 の解答	$\left(\frac{a}{11}\right) = -11$	$\left(\frac{a}{11}\right) = -1$
227	問題 3.17 の解答	$n \equiv 1, 17, \ldots, 53 \pmod{60}$	$n \equiv 1, 2, 4, 8 \pmod{15}$
〃	下から 7 行目と 8 行目	z	ζ
〃	下から 1 行目	$a - \sqrt{m} = 0$	$a - b\sqrt{m} = 0$

頁	行	誤	正
228	問題 4.25 の解答 2 行目	$1-\sqrt{2}$	$1+\sqrt{2}$
〃	下から 1 行目	$\beta' = \alpha'\delta'$	$\beta' = \alpha'\gamma'$
229	下から 2 行目	$(3,1),\ (4,-1-i),\ (4+i,-3i)$	$(3,1),\ (3-i,2i),\ (4,-1-i)$
231	問題 6.10 の解答	$\alpha_i g_k$	$\alpha_i \gamma_k$
232	問題 6.32 の解答 2 行目	$A+B=(1)$ より	$A+B=(1)$ だから
233	下から 6 行目	長岡一明昭	長岡一昭