「代数の世界 改訂版」正誤表　2015.1.

第 1 刷に以下のような誤りがありました．お詫びして訂正いたします．

頁	行	誤	正
3	↑ 5	(1.1)–(1.3)	(1.3)–(1.5)
14	↑ 1	加群	加法群
26	命題 4.10 ↓ 3	$\mathrm{Ker}\,(f) \subseteq H$	$\mathrm{Ker}\,(f) \supseteq H$
29	↑ 1–2	（a と b が公約数を持たないとき）	（a と b が 1 以外の公約数を持たないとき）
32	(5.7.2)	$$\bar{a}=\bar{c},\ \bar{b}=\bar{d} \quad \Rightarrow \\ \overline{a+c}=\overline{b+d},\quad \overline{ac}=\overline{bd}$$	$$\bar{a}=\bar{c},\ \bar{b}=\bar{d} \quad \Rightarrow \\ \overline{a+b}=\overline{c+d},\quad \overline{ab}=\overline{cd}$$
37	問題 1.5. 9.	a と m が素であれば（最大公約数が 1 であるということ）	a と m が互いに素であれば
47	問題 2.1. 11. (1)	$G = U(\mathbb{Z}/(2^k))^*$	$G = U(\mathbb{Z}/(2^k))$
47	問題 2.1. 11. (2)	$G = (\mathbb{Z}/(p^k))^*$	$G = U(\mathbb{Z}/(p^k))$
54	↑ 7, 9	$I \supseteq \mathrm{Ker}\ g$	$I \subseteq \mathrm{Ker}\ g$
71	問題 2.4. 7.	$\bar{f} \in \mathbb{F}_p$	$\bar{f} \in \mathbb{F}_p[X]$
84	(6.1.2)	$$U(A^\Lambda) = \prod_{\lambda\in\Lambda} U(A_\lambda/I_\lambda)$$	$$U(A^\Lambda/I^\Lambda) = \prod_{\lambda\in\Lambda} U(A_\lambda/I_\lambda)$$
88	↑ 3	定理 6.5	定理 6.6
89	↑ 4, 5, 6, 7	加群	加法群
90	定義 7.1 ↓ 1	加群 M が環 A 上の加群	加法群 M が環 A 上の加群
91	↓ 13, 16	加群	加法群（16 行目は「最も簡単な A 加群は加法群としての A に $\cdots$ 」となる.）
91	↑ 3	環 A のイデアルは A 加群.	環 A のイデアルは A の A 部分加群です.
105–106	例 8.6	別紙のように詳細な説明を加えた.	
107	問題 2.8 3. (1)	$\mathbb{Z}/\mathrm{Im}\ f$，$\mathbb{Z}/\mathrm{Im}\ g$	$\mathbb{Z}^2/\mathrm{Im}\ f$，$\mathbb{Z}^2/\mathrm{Im}\ g$
112	↓ 4	$ab \in P,\ a \notin P$ としてみましょう.	$ab \in Q,\ a \notin P$ としてみましょう.　（また,「(1) $\Rightarrow$ P は素イデアル」の証明は別紙を参照.）

頁	行	誤	正
123	$\uparrow 8$	定義 7.12	定理 7.15
133	$\downarrow$ 12–13	**任意の角の 3 等分は作図できない**	**角の 3 等分は一般には作図できない**
136	問題 3.3. 4.	$s(X) = aX + b\ (a, b \in K, a \neq 0)$	$\sigma(X) = aX + b\ (a, b \in K, a \neq 0)$
137	定理 4.1 の証明	証明の最初に「$f(X)$ が既約な場合に示せば十分です.」を追加.	
140	$\downarrow 12$	$g(X) = \tau_L^{-1}(g(X)) \in L[X]$	$g(X) = \tau_L^{-1}(g'(X)) \in L[X]$
142	$\uparrow 11$	$x - \beta$ が $k[X]$ で $f(x)$ を割り切ります.	$x - \beta$ が $K[X]$ で $f(x)$ を割り切ります.
145	$\downarrow 2$	$f'(X) = \sum_{i=1}^n a_i X^{i-1}$	$f'(X) = \sum_{i=1}^n a_i i X^{i-1}$
145	$\uparrow$ 1–2	$\begin{aligned} f(X) &= \sum_{k=1}^{pn_1} a_{pk} X^{pk} \\ &= \sum_{k=1}^{n_1} a_{pk} (X^p)^k = f_1(X^p) \end{aligned}$ (但し $f_1(X) := \sum_{k=1} n_1 a_{pk} X^k$)	$\begin{aligned} f(X) &= \sum_{k=1}^{n_1} a_{pk} X^{pk} \\ &= \sum_{k=1}^{n_1} a_{pk} (X^p)^k = f_1(X^p) \end{aligned}$ (但し $f_1(X) := \sum_{k=1}^{n_1} a_{pk} X^k$)
146	$\downarrow 5$	$f'(X) = ph'(X^p)X^{p-1} = 0$	$f'(X) = p^e h'(X^{p^e})X^{p^e-1} = 0$
155	(6.3)	$\boldsymbol{G}(E) = \{\sigma \in \boldsymbol{G} \mid \sigma(\alpha) = x\ (\forall x \in E)\}$	$\boldsymbol{G}(E) = \{\sigma \in \boldsymbol{G} \mid \sigma(x) = x\ (\forall x \in E)\}$
159	定理 6.8 (b) $\downarrow 2$	$K(\boldsymbol{H}_1) \supset K(\boldsymbol{H}_2) \subset K$	$K(\boldsymbol{H}_2) \subset K(\boldsymbol{H}_1) \subset K$
160	$\uparrow 1$	$\boldsymbol{G}$ は正規部分群	$\boldsymbol{G}(E)$ は正規部分群
178	$\downarrow 3$	$\sigma = \tau_1\tau_2\cdots\tau_k$ と表すとき	$\sigma = \tau_1\tau_2\cdots\tau_k$ と互換の積で表すとき
186	問題 4.3. 6 (1)	「(p は素数とする)」を削除.	
199	問題 4.5. 4.	位数 16 の非同型なアーベル群,非アーベル群の個数に間違いあり.別紙を参照.	
220	$\downarrow 6$	$D(f) = 16.101$	$D(f) = 16 \cdot 101$ (4 次方程式 $X^4 + aX^2 + bX + c = 0$ の判別式は $D(f) = 16a^4c - 4a^3b^2 - 128a^2c^2 + 144ab^2c - 27b^4 + 256c^3$ で与えられる.)
222	$\uparrow 9$	$\langle F^n \rangle \subseteq \langle F^m \rangle$ と $n \mid m$ は同値ですから,	$\langle F^n \rangle \supseteq \langle F^m \rangle$ と $n \mid m$ は同値ですから,

頁	行	誤	正
223	$\uparrow 11$	$\{K[X]$ の既約 n 次主多項式 $\} = \frac{\#T}{n}$	$\sharp\{K[X]$ の既約 n 次主多項式 $\} = \frac{\#T}{n}$
225	問題 5.3. 6. (3) $\downarrow 2$	$fA = a_{14}X^14 + a_{13}X^13 + \cdots + a_1X + a_0$	$fA = a_{14}X^{14} + a_{13}X^{13} + \cdots + a_1X + a_0$
244	問題 2.6.（中国式剰余定理）の解	問題と解答が対応していなかった為，別紙のように訂正.	
247	問題 3.1.（体の拡大）の解	問題と解答が対応していなかった為，別紙のように訂正. また，問題 1.1 (2) の最小多項式を訂正.	
255	問題 5.1.（方程式のガロワ群）**6.**，**7.** の解	**6.** と **7.** の解答を入れ換え.	

例 8.6 例 7.5 を今までやったことを使って解釈しましょう．$A = k[T]$ でした．$L = A^n$ とおき，L の A 上の基底，V の k 上の基底をどちらも $(e_i)_{i=1}^n$ とします．$\phi : L \to V$ を $\phi(\sum f_i(T)e_i) = \sum f_i(u)e_i$ で定義します．ϕ は A 加群の全準同型写像なので，$M = \mathrm{Ker}\,\phi$ は L の A 部分加群です．同型定理より，$V_u \cong L/M$ ですから，この剰余加群の構造を調べるには，$L = A^n$ の部分加群 M の単因子（定理 8.2 参照）が分かればよいことになります．

一方，$u : V \to V$ の基底 $(e_1, \ldots, e_n)$ に関する行列表現を $C = (c_{ij})$ 即ち，

$$u(e_j) = \sum_{i=1}^{n} c_{ij} e_i \tag{8.6.1}$$

とします．同様に $\mu : L \to L$ を (8.6.1) のように $\mu(e_j) = \sum_{i=1}^n c_{ij} e_i$ と定義し，

$$T - \mu : L \to L; \quad (T - \mu)(e_j) = Te_j - \sum_{i=1}^{n} c_{ij} e_i \tag{8.6.2}$$

とおくと，$M = (T - \mu)(L)$ が容易にわかります．

さて，系 8.3 より

$$V_u \cong A/I_1 \oplus \cdots \oplus A/I_s \oplus \underbrace{A \oplus \cdots \oplus A}_{n-s}$$

ですが，k 上の次元を見ると，$\dim_k V_u = n$ で，また $\dim_k k[T] = \infty$ ですから，$n - s = 0$ で V_u は A **加群としてはねじれ加群である**ことが分かります．つまり，$s = n$ で

$$V_u \cong A/I_1 \oplus \cdots \oplus A/I_n.$$

系 8.3 は L の基底 $(e_1, \ldots, e_n)$ をうまく選べば，

$$M = (T - \mu)L = I_1 e_1 \oplus \cdots \oplus I_s e_s \subset L = A^n$$

となることを意味しています．$I_k = (\ell_k(T))$ $(k = 1, \ldots, n)$ とすると，これは $T - \mu$ の行列表現 $TE_n - C$ に対して (E_n は $n \times n$ 単位行列)，A 係数で行列式が A の単元となる n 次正方行列 P, Q があって，

$$P(TE_n - C)Q = \begin{pmatrix} \ell_1(T) & & & 0 \\ & \ddots & & \\ & & \ddots & \\ 0 & & & \ell_n(T) \end{pmatrix} \quad (\ell_1(T) | \cdots | \ell_n(T))$$

となることに他なりません．$\ell_1(T), \ldots, \ell_n(T)$ は行列 $TE_n - C$ の単因子とも云われます．線型代数学より，この単因子は A **係数の行列の基本変形**で得られます．

命題・定義 9.6 の証明 (1) $\Rightarrow$ (2)（$P=\sqrt{Q}$ が素イデアルになること.）

(1) を仮定して，$ab \in P,\ a \notin P$ としてみましょう．定義より $a^n b^n \in Q$ となる n が取れます．a^n は A/Q で巾零でないので，(1) の条件から零因子でもありません．従って $b^n \in Q$，即ち $b \in P$ が云え，P が素イデアルであることが示せました．

問題 4.5

4.

	4	6	8	9	10	12	14	15	16	18	20
アーベル群	2	1	3	2	1	2	1	1	5	2	2
非アーベル群	0	1	2	0	1	3	1	0	9	2	3
計	2	2	5	2	2	5	2	1	14	4	5

問題 2.6（中国式剰余定理）

問題 6.1. (1) P が $A_1 \times A_2$ の素イデアルなら，$(1,0)(0,1)=(0,0)\in P$ より $(1,0)$ または $(0,1)\in P$. $(0,1)\in P$ とすると，$P=P_1\times A_2$ となるのは容易に分かる．

(2) π の λ 成分は自然な全射 $\pi_\lambda : A_\lambda \to A_\lambda/I_\lambda$. $(a_\lambda)\in \operatorname{Ker}\pi$ と $\forall\lambda, a_\lambda \in I_\lambda$ は同値.

問題 6.2. $n=23$. いろいろなやり方を考えよう！

1. $(1-e)(1-e)=1-e-e+e^2=1-e, e(1-e)=0$ に注意．$a=be=c(1-e)$ とすると，両辺に e をかけると $be=0$ より $eA\cap(1-e)A=\{0\}$，$a\in A$ に対し，$a=a.1=a(e+(1-e))=ae+a(1-e)\in eA\times(1-e)A$.

2. $p|n$ なら $\phi(n)\geq p-1$，$p^2|n$ なら $\phi(n)\geq p(p-1)$ 等々で，n の可能性をしぼれる．$\phi(n)\leq 20$ となる最大の n は 66，$\phi(66)=20$，$\phi(n)\leq 50$ となる最大の n は 180，$\phi(180)=48$.

3. Φ が全射で，$\operatorname{Ker}\Phi=(f(a_1),\cdots,f(a_n))$ だから (1) が得られる．(2) は $f=\sum_{i=1}^n b_i f_i$ とすればよい．

4. (1) 前者は位数 8 の元を持つが，後者は持たない．

(2) $\mathbb{F}_2[X]/(X^2)$ で $\bar{X}$ は巾零だが，$\mathbb{F}_2\times\mathbb{F}_2$ は巾零元を持たない．

(3) $A[X,Y]/(XY)\cong \operatorname{Im}\Phi \cong \{(f(X),g(Y))\in A[X]\times A[Y] \mid f(0)=g(0)\}$

問題 3.1（体の拡大）

問題 1.1. 最小多項式は α の満たす既約多項式である．平方根を消去していけば得られる．

(1) x^4-8x^2+36. (2) $x^6-6x^4-6x^3+12x^2-36x+1$.

1. $[K:E]\mid[K:k]<\infty$ より $K/k, K/E$ は代数拡大．α の満たす E 係数既約多項式を $g(X)$，K 係数既約多項式を $f(X)$ とすると，$E[X]$ で $g(X)|f(X)$ である．K に $g(X)$ の係数を添加した体を E' とすれば，$[K:E']=\deg g, E'\subset E$ であるが，$\deg g=[K:E]$ ゆえ $E=E'$ である．従って，中間体は $f(X)$ を $K[X]$ で因数分解したとき，因数となる多項式のいくつかの積の係数を K に添加して得られる．よって，中間体は有限個しかない．

2. $\sqrt{2}$ の $\mathbb{Q}(2^{\frac{1}{3}})$ 上の既約多項式は x^2-2 である．

3. $x\in R, x\neq 0$ に対して，$1,x,x^2,\cdots,x^n$ が K 上線型従属となる最小の正整数 n を取れば，$\exists a_0,a_1,\cdots,a_n\in K$，$a_0\neq 0$ で $a_0+a_1x+\cdots+a_nx^n=0$ となる．これより，x^{-1} は x の多項式ゆえ，$x^{-1}\in R$.（別証明が問題 2.1-**10** にある.）