

数理・情報系のための整数論講義 正誤表

2011年9月13日現在

p.3, 1.4 「 $f(X), g(X) \in R[X]$ がともに零多項式でなければ $\deg(fg) = \deg f + \deg g$ が成り立っている」を次のように訂正. 「 $f(X), g(X) \in R[X]$ がともに零多項式でないとき, $f(X)$ の最高次の係数を a_n , また $g(X)$ の最高次の係数を b_m とすれば $f(X)g(X)$ の最高次の係数は a_nb_m になる. したがって $a_nb_m \neq 0$ であれば $\deg(fg) = \deg f + \deg g$ が成り立つ. 特に R が整域 (次の定義 1.4) の場合はこの等式が成り立つ」

定義 2.4 「 a_1, \dots, a_n を 0 でない整数とする」を 「 a_1, \dots, a_n を少なくともひとつは 0 でない整数とする」

問題 4.4 $I_1 + I_2 := \{a_1 + a_2 \mid a_1 \in I_1, a_2 \in I_2\}$

定義 4.6 「イデアル I が」を 「イデアル $I (\neq R)$ が」に. 「 $a, b \in I$ に対して」を 「 $a, b \in R$ に対して」に.

系 5.12 始めの方を 「 \mathbb{Z} および $K[X]$ の (0) でない素イデアルと」に変更.

補題 6.2, 1.5 $|c| = c(f)$

補題 6.2 証明の下から 2 行目 $c(cf_0) = |c|, c(dg_0) = |d|$

p.20, 1.1 $\sum_{j=0}^i b_j c_{i-j}$

p.20 第 7 節の第一文 「 $I (\neq R)$ を R のイデアルとする」に変更.

p.21 命題 7.4 1.1 $a \in R$

p.24 定理 7.10 の証明の後 厳密には次のように書きかえるべき. 「 \mathbb{Z} の (0) でないイデアルについて、素イデアルになることと極大イデアルになることは同じであった (系 5.12). したがって $m > 1$ のとき剰余環 $\mathbb{Z}/m\mathbb{Z}$ が....」

定義 8.1 (iv) 「 $a * b = a * b$ 」を 「 $a * b = b * a$ 」に.

定義 8.7 「 $\varphi(m)$ と書く。」の後に 「ただし $\varphi(1) = 1$ と定義する。」を挿入.

定理 9.12 の直前 $a \equiv b \pmod{N}$

定理 9.12 の証明の後半 でてくる H をすべて N に.

補注 10.3 最初に次の文を挿入, 「補注 6.1 での注意を一般にすると係数が整域にあればモニックな多項式に対して因数定理 (系 3.3) が成立する. したがって,」

補注 10.8 「無数にあるだろうか」を「無数にある」に.

例 11.7 $f(X)$ を次のようにする. $f(X) = X^5 + 2X^4 + 6X^3 + X^2 + 11$. すると $\bar{f}(X) = X^5 + X^2 + 1$ になる. この \bar{f} は $X^2 + X + 1$ でわれない.

もとの f も実は $\mathbb{Q}[X]$ で既約である. それを示すには $p = 5$ ととればよい. ただし同じ方法で示そうとするなら $\mathbb{F}_5[X]$ の既約な 2 次式は

$$\begin{array}{lll} X^2 + 4X + 2, & X^2 + 3X + 4, & X^2 + 3, \\ X^2 + 4X + 1, & X^2 + 3X + 3, & X^2 + X + 1, \\ X^2 + 2, & X^2 + X + 2, & X^2 + 2X + 4, \\ X^2 + 2X + 3 & & \end{array}$$

の 10 個あるのでそれぞれでわってみなければならぬ.

命題 12.5, 系 13.6 (Euler function, Euler's totient function) を削除. これは元原稿にはなく, index に入れるために編集者が誤挿入したものであると思われ.

命題 12.5 (ii) 文頭に 「 p が素数なら」を追加.

命題 12.5 (ii) 「 m の因数分解」を「 n の因数分解」に.

系 13.6 の証明 「問題 13.3 (iii) の式」を「問題 13.3(iii) から得られる式」に.

命題 14.2 の 1.5 「である」を「が解を持つことである」に.

定理 14.3 「ここで p は素数で, f の最高次の係数をわらないとする」の後に次の文を追加. 「ただし $g(X) \pmod{p}$ は $g(X)$ の係数を法 p で考え, $\mathbb{Z}/p\mathbb{Z}$ 係数の多項式と考えたものをあらわす.」

命題 15.2 「オイラーの基準」を「オイラーの規準」に. 前者を使っている本もあるのですが, 数学辞典にあわせてこのようにします.
pp.56,70,73,90,146,202,203,210 にもあります.

定理 17.5 証明の後半が正しくないので次のように変更します.

逆を証明する. $2 = g(1, 1)$ だから問題がないので, p を奇素数とする. $p \equiv 1 \pmod{4}$ なら $p = 4k + 1$ とかける. フェルマーの小定理(系 9.9) から

$$(X^{2k} - 1)(X^{2k} + 1) = X^{4k} - 1 \equiv 0 \pmod{p}.$$

多項式 $X^{2k} - 1 \in \mathbb{F}_p[X]$ は命題 10.2 から \mathbb{F}_p 内に高々 $2k < p$ 個しか根を持たないから, $X^{2k} - 1 \not\equiv 0 \pmod{p}$ となる $X \in \mathbb{Z}$ がある. この X に対して $X^{2k} + 1^2 \equiv 0 \pmod{p}$ である. したがって定理を証明するには次の補題を証明すればよい.

命題 20.2 のあと 式 (20.3) のあとを次のように変更.

「 $(n', p - 1) = 1$ ならば n' 乗写像が全単射になるから, ... 帰着されることになる.」 「以下ではこの $p \equiv 1 \pmod{n}$ の場合だけを考える.」

命題 23.16 2 行目の $\text{Gal}(KL/L)$ を $\text{Gal}(KL/k)$ に訂正.

p.111 (25.3) が同型である証明ができていませんので, このページの初めから定理 25.5 の前までを次のように変更.

次に $\Phi_n(X)$ が $\mathbb{Q}[X]$ の既約多項式であることを証明する. $u(X) = \text{Irr}(\zeta_n, \mathbb{Q}; X)$ とすると, $u(X) | X^n - 1$ より $X^n - 1 = u(X)v(X)$ と書ける. ここで $v(X) \in \mathbb{Q}[X]$ であるが $u(X), v(X)$ はともにモニックだから, 定理 6.4 の証明より $u(X), v(X) \in \mathbb{Z}[X]$ となっている.

p を n をわらない素数とする. このとき 1 の n 乗根 ζ が $u(X)$ の根ならば $u(\zeta^p) = 0$ であることを示そう. そのために $u(\zeta^p) \neq 0$ と仮定して矛盾を出す. $u(\zeta^p)v(\zeta^p) = (\zeta^n)^p - 1 = 0$ から ζ^p は $v(X)$ の根, したがって ζ は $v(X^p)$ の根になる. $u(X)$ は既約だから ζ の最小多項式でもあるから $u(X) | v(X^p)$. ともにモニックな整多項式であることに注意すると, ある $w(X) \in \mathbb{Z}[X]$ を使って $v(X^p) = u(X)w(X)$

と書ける. v, u, w を $\text{mod } p$ した多項式をそれぞれ $\bar{v}, \bar{u}, \bar{w}$ と書くと (命題 11.6 参照),

$$\bar{v}(X)^p = \bar{v}(X^p) = \bar{u}(X)\bar{w}(X)$$

が $\mathbb{Z}/p\mathbb{Z}[X]$ で成り立つ. ここで最初の等式は問題 18.3 と同じ理由により成立する. この式から $\bar{u}(X)$ の既約因子は $\bar{v}(X)$ の既約因子にもならなくてはならない. これから $\bar{u}(X)$ と $\bar{v}(X)$ は共通根を持つ. したがって $X^n - 1 \pmod{p}$ は重根を持たなければいけないが, これは付録 A の系 A.6 と問題 A.2 により $D(X^n - 1) \equiv 0 \pmod{p}$ となるので不可能である. よって $u(\zeta^p) = 0$.

さてここで ζ_n^j を任意の原始 n 乗根とし, $j = p_1 \cdots p_t$ を j の素因数分解とする. このとき $(n, j) = 1$ より $(n, p_i) = 1$ ($i = 1, \dots, t$) である. 上で証明したことを繰り返し使うと ζ_n が $u(X)$ の根であることから $\zeta_n^{p_1}, \zeta_n^{p_1 p_2}, \dots, \zeta_n^{p_1 p_2 \cdots p_t} = \zeta_n^j$ も $u(X)$ の根になる. つまり任意の原始 n 乗根は $u(X)$ の根となる.

以上により ζ_n の \mathbb{Q} 上の共役は ζ_n^j ($(j, n) = 1$) の全体になるから, $i \in (\mathbb{Z}/n\mathbb{Z})^*$ に対して σ_i を $\zeta_n \mapsto \zeta_n^i$ で定めると, これは C_n の \mathbb{Q} 上の自己同型になって, 写像

$$f: (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \text{Gal}(C_n/\mathbb{Q}), \quad i \mapsto \sigma_i \quad (25.3)$$

が定まる. この写像は簡単にわかるように群の準同型写像になっている. さらに $\sigma_i = \text{id}$ となるのは $i \equiv 1 \pmod{n}$ の時であるから, この準同型は単射である. また上で示したことから

$$\text{Irr}(\zeta_n, \mathbb{Q}; X) = \Phi_n(X) \quad (25.4)$$

であるから $[C_n : \mathbb{Q}] = \varphi(n)$ だから (25.3) の準同型は同型である. 以上より次の定理が得られた.

定理 29.3 の証明 p.134 の真ん中あたり. 「次に」以降を段落の最後までを次のようにする. 「次に $\sum_{i=1}^m c_i \omega_i = 0$ ($c_i \in k$) とする. 両辺に適当な 0 でない有理整数をかけて $c_i \in \mathcal{O}_k$ としてよい. ここで I を c_1, \dots, c_m によって生成される \mathcal{O}_k のイデアルとする. $I \subset \mathfrak{p}$ である. ここで, もし $I \neq (0)$ なら, $xI \not\subset \mathfrak{p}$ をみたす $x \in I^{-1}$ が存在する. 実際すべての $x \in I^{-1}$ について $xI \subset \mathfrak{p}$ なら $\mathcal{O}_k = I^{-1}I \subset \mathfrak{p}$ と

なり矛盾である. x の取り方から, ある j について $xc_j \notin \mathfrak{p}$ だが, I^{-1} の定義からすべての i に対して $xc_i \in \mathcal{O}_k$ である. はじめの式にこの x をかけて, $\sum_{i=1}^m xc_i\omega_i = 0$ を得る. この式を $\text{mod } \mathfrak{p}$ で考えると, $xc_j \notin \mathfrak{p}$ から ω_i たちの $\mathcal{O}_k/\mathfrak{p}$ 上の自明でない線形関係式が得られる. これは ω_i たちが $\mathcal{O}_k/\mathfrak{p}$ 上で一次独立であることに反する. したがって $I = (0)$. すなわち, $c_i = 0$ がすべての i について成り立つ. 以上から ω_i たちは K/k の基底になるので, $m = [K:k] = n$ で $\dim_{\mathcal{O}_k/\mathfrak{p}}(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K) = n$ がわかった.]

補注 31.10 1.4-5 p が分解体でも不分岐になることの証明を次のようにする.

「 α を $f(X)$ の根とすると, $\sigma \in D(p)$ に対して, $\sigma(\alpha)$ も $f(X)$ の根である. このとき $\sigma \in I(p)$ なら $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}$ となる. 一方, 仮定から, $p \nmid D(f)$ により, f が $\text{mod } p$ で重根をもたない. したがって $\sigma = 1$ がわかる. このとき (31.3) から.....」

命題 34.3 の証明 $S \cap L$ の元が有限個であることを示したあと, 「そこで」からその次の行の「と書く」までを次のように訂正.

「そこで $S \cap L$ の元の中で $|r_n|$ が最小正の数になるような元を w_n とする. $w_n \notin W$ より w_1, \dots, w_n は V の基底になる. このとき $L = \mathbb{Z}w_1 + \dots + \mathbb{Z}w_n$ となることを示そう. w_n の選び方から, このとき $\mathbb{Z}w_1 + \dots + \mathbb{Z}w_n \subset L$ が明らかに.....」

証明の最後から 5 行目 $0 \leq q < 1$ に訂正.

証明の最後から 3 行目 $0 \leq q|r_n| < |r_n|$ に訂正.

定理 35.1 の証明 p.161 の $\text{vol}(B_c)$ の式の π のべきが間違い.

$$\text{vol}(B_c) = \frac{2^{r_1-r_2}\pi^{r_2}c^n}{n!}$$

p.201 **問題 12.1 の解答** 1664 を 1668 に.

p.111, p.150 など アーベル拡大のあとの (abelian extension) をとる. これも元原稿にありません. 術語の英訳は目次だけにあるのがデフォルトです.

数学者名及び生没年一覧 ガロア Évariste Galois 1811-1832 を追加. 生年順にソートするのを忘れてました.

この正誤表を作るにあたって次の方々の御指摘を参考にさせていただきました。ここにお名前をあげて感謝します。
山岸正和さん，福田隆さん，田谷久雄さんおよび宮城教育大田谷卒研ゼミのみなさん，中野伸さん，山崎隆雄さん。