一変数多項式の分解法則

1. 基本問題

$u(X)$ を既約、モニックな $\mathbb{Z}$ 上の多項式とする。$u(X)$ を $\mathbb{F}_p$ 上考えたときの分解は p によりどう変わるか?

```
p:X^2-5;
modulus:7;
for i:1 thru 10 do
block(modulus:next_prime(modulus), print([modulus,factor(p)]));

[11, (X - 4) (X + 4)]
      2
[13, X  - 5]
      2
[17, X  - 5]
[19, (X - 9) (X + 9)]
      2
[23, X  - 5]
[29, (X - 11) (X + 11)]
[31, (X - 6) (X + 6)]
      2
[37, X  - 5]
[41, (X - 13) (X + 13)]
      2
[43, X  - 5]
```

別の多項式

```
      5
[11, X  - X - 1]
      5
[13, X  - X - 1]
                       3      2
[17, (X - 8) (X - 6) (X  - 3 X  - 5 X + 6)]
           2   3      2
[19, (X + 6)  (X  + 7 X  - 6 X - 9)]
              4      3       2
[23, (X + 9) (X  - 9 X  - 11 X  + 7 X + 5)]
              4      3      2
[29, (X - 2) (X  + 2 X  + 4 X  + 8 X - 14)]
              4      3      2
[31, (X + 2) (X  - 2 X  + 4 X  - 8 X + 15)]
       2              3       2
[37, (X  + 16 X - 8) (X  - 16 X  + 5 X + 14)]
                       3      2
[41, (X - 8) (X + 15) (X  - 7 X  + 5 X - 14)]
                       3       2
[43, (X - 18) (X - 9) (X  - 16 X  + 8 X + 13)]
```

2. 詳しい設定

K を $\mathbb{Q}$ の有限次 Galois 拡大とする。K は $\mathbb{Q}$ 上の単拡大であるから、その生成元の一つ α の最小多項式 $u(X)$ をとって、

$$K = \mathbb{Q}[X]/(u(X))$$

必要ならば α を取り替えて、$u \in \mathbb{Z}[X]$ かつ u は monic としてよい。

$R = \mathbb{Z}[X]/(u(X))$ と書くと、$K = Q(R)$ である。

$\mathrm{Gal}(K/\mathbb{Q})$ を以下では G と書くことにする。

2.1. r_σ**.** $\sigma \in G$ にたいして、$\sigma(\alpha) \in K$ であるから、$\exists r_\sigma(X) \in \mathbb{Q}[X]$ で、

$$\boxed{\sigma(\alpha) = r_\sigma(\alpha).}$$

一般の $p(X) \in \mathbb{Q}[X]$ に対して、$\sigma(p(\alpha)) = p(\sigma(\alpha))$ である。

以下では、$\sigma \in G$ にたいして、$\sigma(\alpha)$ のことを α_σ とも書くことにする。u の根は $\{\alpha_\sigma; \sigma \in G\}$ である。

2.2. p **で切る。.** $p \in \mathrm{Spm}(\mathbb{Z})$ をとり、p 上 R は不分岐であるとする。(有限個の p を除き、この不分岐性の仮定は満たされる。) (p) 上の $\mathrm{Spm}(R)$ の元を $\{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s\}$ とおく。これをもう少し詳しく説明しよう。$R/pR \cong \mathbb{F}_p[X]/(u(X))$ であり、$\mathbb{F}_p$ 上 u の既約分解を

$$\bar{u} = \bar{u}_1 \bar{u}_2 \ldots \bar{u}_s \qquad (/\mathbb{F}_p)$$

とする。不分岐性の仮定により、$\bar{u}$ は $\mathbb{F}_p$ 上重根をもたない。

$$(2.1)\quad R \otimes \mathbb{F}_p \cong \mathbb{Z}[X]/(p, u(X)) \cong \mathbb{F}_p[X]/(u(X)) \cong \prod_{j=1}^{s} \mathbb{F}_p[X]/(\bar{u}_j(X))$$

$\bar{u}_j \in \mathbb{F}_p[X]$ は仮定により既約であるから、最後の $\mathbb{F}_p[X]/(\bar{u}_j)$ は体であり、したがって $\mathfrak{p}_j = (p, u_j(\alpha))$ は $R \otimes \mathbb{F}_p$ の素イデアルである。

補題 2.1. G は $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ に transitive に作用する。

Proof. 付値の独立性からである。R の元 f_j で S の一点 $\mathfrak{p}_j$ でのみ値が 1, その他の S の点では値が 0 をとるようなものをとると、それらは Galois 群の元で互いに移りあわねばならない。($\sum_\sigma \sigma(f_1)$ は G-invariant ゆえ $\mathbb{Z}$ の元で、それゆえ $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_s$ での値が全て等しい。) □

$\mathfrak{p} = \mathfrak{p}_1$ とおき、$H = \{\sigma \in G; \sigma(\mathfrak{p}) = \mathfrak{p}\}$ ($\mathfrak{p}$ の分解群) とおく。

2.1 式により、

$$\deg(u) = \sum_j \deg \bar{u}_j = \sum_j [R/\mathfrak{p}_j : \mathbb{F}_p].$$

transitivity により、$[R/\mathfrak{p}_j : \mathbb{F}_p]$ は j に依らない。よって、

$$|G| = \deg(u) = s \cdot [R/\mathfrak{p} : \mathbb{F}_p].$$

他方、$|G| = |H|s$ であるから、結局

$$|H| = [R/\mathfrak{p} : \mathbb{F}_p]$$

さて、制限から決まる群準同型 $\mathrm{restr} : H \to \mathrm{Gal}((R/\mathfrak{p})/\mathbb{F}_p)$ を考えよう。

補題 2.2. restr は 全単射 (よって同型) である。

Proof. 位数が等しい群の間の準同型であるから、単射であることを示せば十分である。$\sigma \in \mathrm{Ker}(\mathrm{restr})$ を考える。$\sigma(\mathfrak{p}) = \mathfrak{p}$ でありかつ σ は $R/\mathfrak{p}$ の上で恒等写像と一致する。よって σ は completion $R_\mathfrak{p}$ の上で恒等写像を誘導し、改めて R に制限すると $\sigma = \mathrm{id}$. □

系 2.3. G の元 σ で、 $\sigma(\mathfrak{p}) = \mathfrak{p}$ かつ σ が $R/\mathfrak{p}$ に誘導する写像がちょうど $R/\mathfrak{p}$ の Frobenius 自己同型 frob と等しいものが一意に存在する。[これを $\mathrm{Frob}_{\mathfrak{p}}$ と書く。]

frob は (標数 p の環の間の) 環準同型と可換であるから、$\tau \in G$ にたいして、 $R/\mathfrak{p}$ から $R/\tau(\mathfrak{p})$ への環準同型として $\tau \circ \mathrm{frob} = \mathrm{frob} \circ \tau$. $R/\tau(\mathfrak{p})$ の環自己同型として

$$\mathrm{frob} = \tau \circ \mathrm{frob} \circ \tau^{-1}$$

である。これらを induce する環準同型を調べれば、

Frob の conjugation

$$\mathrm{Frob}_{\tau(\mathfrak{p})} = \tau \circ \mathrm{Frob}_{\mathfrak{p}} \circ \tau^{-1}$$

が従う。

注意:

- $\alpha_1, \ldots, \alpha_s$ は $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ 上の関数と考えるべきである。
- 「$\alpha_i \mod p$」 のようなものはいきなりは定義できない。例えば $u(X) = X^2 + 1 = (X + \sqrt{-1})(X - \sqrt{-1})$ の modulo 5 での様子を考えてみよ。($\mathbb{F}_5$ 上では $(X^2 + 1) = (X - 2)(X + 2)$ だが、$2, -2$ のどちらが $\sqrt{-1}$ modulo 5 の値であるとも言えない。このあたりの感触はいかにも Galois 理論的である。) p の lift $\mathfrak{p}_1$ を確定すれば、α_1 の modulo $\mathfrak{p}$ の値も確定するわけである。

問題 2.1. $\sigma_1 = \mathrm{Frob}_{\mathfrak{p}_1}$ が既知であるとして、$u_1, u_2, \ldots, u_s$ と、Frobenius 元 $\sigma_1, \ldots, \sigma_s$ ($\sigma_j \stackrel{\mathrm{def}}{=} \mathrm{Frob}_{\mathfrak{p}_j}$) をもとめ、さらに、$r_p$ を求めよ。

分解群 H は $\mathrm{Frob}_{\mathfrak{p}_1}$ で生成されるから、$H = \langle \sigma_1 \rangle$ である。G/H の代表元を $\tau_1, \tau_2, \ldots, \tau_s$ とおくと、(必要なら添字のとり方を取り替えれば) $\tau_j(\mathfrak{p}_1) = \mathfrak{p}_j$ である。Frob の conjugation に関する主張により、

$$\sigma_j = \tau_j \sigma_1 \tau_j^{-1}$$

H は可換であるからこれらは代表元 τ_j のとり方に依らず well-defined である。

$$u_j \stackrel{\mathrm{def}}{=} \prod_{\sigma \in H} (X - \sigma\tau_j^{-1}(\alpha))$$

とおく。これはやはり 代表元 τ_j のとり方に依らず、$\tau_j H \in G/H$ のみに依る。G の modulo H による分解により、

$$u = \prod_{j=1}^{s} u_j.$$

一般に、$x \in R$ に対して x modulo $\mathfrak{p}_j$ のことを ($[x]_{\mathfrak{p}_j}$ を更に略して) $[x]_j$ と書くことにする。

($\mathfrak{p}_1$ 上の分解)
$$[u]_1 = \prod_j [u_j]_1$$

$$[u_j]_1 = \prod_{\sigma \in H} (X - \sigma\tau_j^{-1}(\alpha))$$

で、これの各係数は $R/\mathfrak{p}_1$ の H-invariant な元であるから、$\mathbb{F}_p$ 係数であることがわかる。すなわち ($\mathfrak{p}_1$ 上の分解) 式は u modulo p の $\mathbb{F}_p$ での素因数分解を与えている。

$$r_p(X) = \sum_k \frac{u(X)}{(X - \alpha_k)u'(\alpha_k)} \alpha_k^p$$

$$r_p(X) \equiv \sum_k \frac{u(X)}{(X-\alpha_k)u'(\alpha_k)}\sigma_1(\alpha_k) \pmod{\mathfrak{p}_1}$$

$$r_p(X) \equiv \sum_k \frac{u(X)}{(X-\alpha_k)u'(\alpha_k)}\sigma_1(\alpha_k) \pmod{\mathfrak{p}_1}$$

他方、$R/\mathfrak{p}_j$ 地点で考えると、対応 $\tau_j : R/\mathfrak{p} \to R/\mathfrak{p}_j$ により、$[u_j]_1$ に対応するのは

$$[\tau_j.u_j]_j = \prod_{\sigma\in H_j}(X - \sigma([\alpha]_j))$$

であるから、これは $[\alpha]_j$ を根として持つ $\mathbb{F}_p$ 係数の多項式である。いいかえれば、$[\alpha]_j$ の $\mathbb{F}_p$ 上の最小多項式である。そこで $\mathfrak{p}_j = (p, u_j(\alpha))$ がわかる。

$$r_p(X) \equiv \sum_k \frac{u(X)}{(X-\alpha_k)u'(\alpha_k)}\sigma_1(\alpha) \pmod{(p, \overline{u_1})}$$

これを j についても同じことを行えば、r_p の御姿が得られる。

3

u の discriminant の素因子は有限個で、それらは個別に考えることにする。以下、それらの p を除外する。環として $\mathbb{F}_p[T]/(u(T))$ は $\mathbb{F}_p$ の有限次代数拡大体の直積である。そこへの Frobenius action を同定すること、これが問題である。

T^p を $\mathbb{Z}$ 上の多項式として $u(T)$ で割ったあまりを $r_p(T)$ とおく。

$$\mathbb{F}_p[T] \ni f(T) \mapsto f(r_p(T)) \in \mathbb{F}_p[T]$$

は $\mathbb{F}_p[T]/(u(T))$ の環自己同型をあたえる。r_p の周期点の個数から $\mathbb{F}_p[T]/(u(T))$ (有限体の直積と同型) の構造がわかる。

r_p を式で表すには黒岩さんとの研究で補完式を用いれば良いことが結論されている:

$$r_n(x) = \sum_{j=1}^{d} \alpha_j^n \frac{u(x)}{u'(\alpha_j)(x-\alpha_j)}.$$

分解法則は、次の関数の $z = p$ での値で決まる:

$$\exp(2\pi\sqrt{-1}r_z(x)/z) = \exp\left(2\pi\sqrt{-1}\sum_{j=1}^{d}\frac{\alpha_j^z}{z}\frac{u(x)}{u'(\alpha_j)(x-\alpha_j)}\right).$$

α_j^z は $\log(\alpha_j)$ のとり方できまり、したがって、上の関数は根の置換による作用を受ける。さて、上の関数には見かけ上 pole があるが、

$$r_0(x) = \sum_{j=1}^{d}\frac{u(x)}{u'(\alpha_j)(x-\alpha_j)}$$

は 各 α_j において 1 を取るような多項式であり、次数の関係から、$r_0(x) = 1$. したがって

$$\exp(2\pi\sqrt{-1}\left(\frac{r_z(x)}{z}\right)) = \exp(2\pi\sqrt{-1}\left(\frac{r_z(x)-r_0(x)}{z}\right))$$

$$= \exp\left(2\pi\sqrt{-1}\sum_{j=1}^{d}\frac{\alpha_j^z-1}{z}\frac{u(x)}{u'(\alpha_j)(x-\alpha_j)}\right).$$

よって、これは立派な z の正則関数である。