教育課題演習　第 10 回　ガロア体 GF(2^m)

１．共役根

m を正の整数とするとき，GF(2)上の m 次既約多項式の根 α を利用して 2^m 個の要素からなる GF(2)の拡大体が作れる。α は原始根であり，$\alpha^{2^m-1}=1$ である。この体を GF(2^m)で表す。

$P(x)$を GF(2)の要素を係数とする多項式とするとき，$P(\beta)=0, P(\gamma)=0$ となる GF(2^m)の要素 β, γ を共役根という。

$P(x)=a_0+a_1x+a_2x^2+\cdots a_nx^n$ $(a_0,a_1,a_2,\cdots,a_n\in GF(2))$に対し $P(\beta)=0$ であるとすると，

$$a_0^2=a_0,\ a_1^2=a_1,\ a_2^2=a_2,\cdots,\ a_n^2=a_n,$$

$$(a_0+a_1\beta+a_2\beta^2+\cdots a_n\beta^n)^2=a_0^2+(a_1\beta)^2+(a_2\beta^2)^2+\cdots+(a_n\beta^n)^2+2(a_0a_1\beta+a_0a_2\beta^2+\cdots)$$

$$=a_0+a_1\beta^2+a_2(\beta^2)^2+\cdots+a_n(\beta^2)^n$$

だから，$P(\beta^2)=0$。

すなわち，β が $P(x)$の根であれば，β^2 は共役根である。

同様に，β が $P(x)$の根であれば，$\beta^2, \beta^4, \beta^8,\cdots$も共役根である。

２．$x^{2^m-1}-1$ の因数分解

α は GF(2^m)の原始根で，$\alpha^{2^m-1}=1$ であるとする。

$(\alpha^2)^{2^m-1}=(\alpha^{2^m-1})^2=1$，$(\alpha^3)^{2^m-1}=(\alpha^{2^m-1})^3=1$，……

より，$1, \alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2^m-1}$ は $x^{2^m-1}-1$ の根であるので，因数定理を用いると，

$$x^{2^m-1}-1=(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)\cdots(x-\alpha^{2^m-2})$$

共役根を含む因数をまとめると GF(2)上既約な多項式の積の形に変形できる。

(1) $x^3-1=(x-1)(x^2+x+1)=(x+1)(x^2+x+1)$

(2) x^7-1 の因数分解

α を $1+x+x^3$ の根とする。

$\alpha^7=1$ より，$\alpha^8=\alpha$ なので，α の共役根は，α^2，α^4 であり，$x^3+x+1=(x-\alpha)(x-\alpha^2)(x-\alpha^4)$

つぎに，α^3 の共役根を求める。$(\alpha^3)^2=\alpha^6$，$(\alpha^3)^4=\alpha^{12}=\alpha^5$，$(\alpha^3)^8=\alpha^{24}=(\alpha^7)^3\alpha^3=\alpha^3$ なので，$(x-\alpha^3)(x-\alpha^6)(x-\alpha^5)$が α^3 の共役根を持つ多項式。

$$(x-\alpha^3)(x-\alpha^6)(x-\alpha^5)=x^3-(\alpha^3+\alpha^6+\alpha^5)x^2+(\alpha^3\alpha^6+\alpha^6\alpha^5+\alpha^5\alpha^3)x-\alpha^3\alpha^6\alpha^{12}$$

$$=x^3-\{(\alpha^3+(1+\alpha)\alpha^5)\}x^2+(\alpha^9+\alpha^{11}+\alpha^8)x-\alpha^3\alpha^6\alpha^{12}$$

$$=x^3-(\alpha^3+\alpha^8)x^2+(\alpha^2+\alpha^4+\alpha)x-\alpha^{21}$$

$$=x^3-(\alpha^3+\alpha)x^2+\alpha(1+\alpha+\alpha^3)x-1$$

$$=x^3-(1+\alpha+\alpha)x^2+\alpha(1+\alpha+\alpha^3)x-1$$

$$=x^3+x^2+1$$

$x^7-1=(x-1)(x-\alpha)(x-\alpha^2)\ (x-\alpha^3)\ (x-\alpha^4)\ (x-\alpha^5)\ (x-\alpha^6)$

$=$