付 録A　ガロア拡大体$\mathbf{GF}(2^m)$

A.1　ガロア拡大体$\mathbf{GF}(2^8)$のべき表現とベクトル表現

1. 原始多項式 (既約多項式) は $x^8+x^4+x^3+x^2+1$ とする ($\alpha^8=\alpha^4+\alpha^3+\alpha^2+1$)。
   なお、$\alpha^{2^8-1}\equiv\alpha^{255}\equiv\alpha^0\equiv 1 \bmod (\alpha^8+\alpha^4+\alpha^3+\alpha^2+1)$ より、$\alpha^{255}=1$。
2. 多項式の係数は 2 を法とする (mod 2)。

べき	展開	ベクトル
α^0	1	00000001
α^1	α	00000010
α^2	α^2	00000100
α^3	α^3	00001000
α^4	α^4	00010000
α^5	α^5	00100000
α^6	α^6	01000000
α^7	α^7	10000000
α^8	$\alpha^4+\alpha^3+\alpha^2+1$	00011101
α^9	$\alpha^5+\alpha^4+\alpha^3+\alpha$	00111010
α^{10}	$\alpha^6+\alpha^5+\alpha^4+\alpha^2$	01110100
α^{11}	$\alpha^7+\alpha^6+\alpha^5+\alpha^3$	11101000
α^{12}	$\alpha^7+\alpha^6+\alpha^3+\alpha^2+1$	11001101
α^{13}	$\alpha^7+\alpha^2+\alpha+1$	10000111
α^{14}	$\alpha^4+\alpha+1$	00010011
α^{15}	$\alpha^5+\alpha^2+\alpha$	00100110
α^{16}	$\alpha^6+\alpha^3+\alpha^2$	01001100
α^{17}	$\alpha^7+\alpha^4+\alpha^3$	10011000
α^{18}	$\alpha^5+\alpha^3+\alpha^2+1$	00101101
α^{19}	$\alpha^6+\alpha^4+\alpha^3+\alpha$	01011010
α^{20}	$\alpha^7+\alpha^5+\alpha^4+\alpha^2$	10110100
α^{21}	$\alpha^6+\alpha^5+\alpha^4+\alpha^2+1$	01110101
α^{22}	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha$	11101010
α^{23}	$\alpha^7+\alpha^6+\alpha^3+1$	11001001
α^{24}	$\alpha^7+\alpha^3+\alpha^2+\alpha+1$	10001111
α^{25}	$\alpha+1$	00000011
α^{26}	$\alpha^2+\alpha$	00000110
α^{27}	$\alpha^3+\alpha^2$	00001100
α^{28}	$\alpha^4+\alpha^3$	00011000
α^{29}	$\alpha^5+\alpha^4$	00110000
α^{30}	$\alpha^6+\alpha^5$	01100000
α^{31}	$\alpha^7+\alpha^6$	11000000

べき	展開	ベクトル
α^{32}	$\alpha^7+\alpha^4+\alpha^3+\alpha^2+1$	10011101
α^{33}	$\alpha^5+\alpha^2+\alpha+1$	00100111
α^{34}	$\alpha^6+\alpha^3+\alpha^2+\alpha$	01001110
α^{35}	$\alpha^7+\alpha^4+\alpha^3+\alpha^2$	10011100
α^{36}	$\alpha^5+\alpha^2+1$	00100101
α^{37}	$\alpha^6+\alpha^3+\alpha$	01001010
α^{38}	$\alpha^7+\alpha^4+\alpha^2$	10010100
α^{39}	$\alpha^5+\alpha^4+\alpha^2+1$	00110101
α^{40}	$\alpha^6+\alpha^5+\alpha^3+\alpha$	01101010
α^{41}	$\alpha^7+\alpha^6+\alpha^4+\alpha^2$	11010100
α^{42}	$\alpha^7+\alpha^5+\alpha^4+\alpha^2+1$	10110101
α^{43}	$\alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha+1$	01110111
α^{44}	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha$	11101110
α^{45}	$\alpha^7+\alpha^6+1$	11000001
α^{46}	$\alpha^7+\alpha^4+\alpha^3+\alpha^2+\alpha+1$	10011111
α^{47}	$\alpha^5+\alpha+1$	00100011
α^{48}	$\alpha^6+\alpha^2+\alpha$	01000110
α^{49}	$\alpha^7+\alpha^3+\alpha^2$	10001100
α^{50}	α^2+1	00000101
α^{51}	$\alpha^3+\alpha$	00001010
α^{52}	$\alpha^4+\alpha^2$	00010100
α^{53}	$\alpha^5+\alpha^3$	00101000
α^{54}	$\alpha^6+\alpha^4$	01010000
α^{55}	$\alpha^7+\alpha^5$	10100000
α^{56}	$\alpha^6+\alpha^4+\alpha^3+\alpha^2+1$	01011101
α^{57}	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha$	10111010
α^{58}	$\alpha^6+\alpha^5+\alpha^3+1$	01101001
α^{59}	$\alpha^7+\alpha^6+\alpha^4+\alpha$	11010010
α^{60}	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+1$	10111001
α^{61}	$\alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha+1$	01101111
α^{62}	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha$	11011110
α^{63}	$\alpha^7+\alpha^5+1$	10100001

べき	展開	ベクトル
α^{64}	$\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha+1$	01011111
α^{65}	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha$	10111110
α^{66}	$\alpha^6+\alpha^5+1$	01100001
α^{67}	$\alpha^7+\alpha^6+\alpha$	11000010
α^{68}	$\alpha^7+\alpha^4+\alpha^3+1$	10011001
α^{69}	$\alpha^5+\alpha^3+\alpha^2+\alpha+1$	00101111
α^{70}	$\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha$	01011110
α^{71}	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^2$	10111100
α^{72}	$\alpha^6+\alpha^5+\alpha^2+1$	01100101
α^{73}	$\alpha^7+\alpha^6+\alpha^3+\alpha$	11001010
α^{74}	$\alpha^7+\alpha^3+1$	10001001
α^{75}	$\alpha^3+\alpha^2+\alpha+1$	00001111
α^{76}	$\alpha^4+\alpha^3+\alpha^2+\alpha$	00011110
α^{77}	$\alpha^5+\alpha^4+\alpha^3+\alpha^2$	00111100
α^{78}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3$	01111000
α^{79}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4$	11110000
α^{80}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$	11111101
α^{81}	$\alpha^7+\alpha^6+\alpha^5+\alpha^2+\alpha+1$	11100111
α^{82}	$\alpha^7+\alpha^6+\alpha^4+\alpha+1$	11010011
α^{83}	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha+1$	10111011
α^{84}	$\alpha^6+\alpha^5+\alpha^3+\alpha+1$	01101011
α^{85}	$\alpha^7+\alpha^6+\alpha^4+\alpha^2+\alpha$	11010110
α^{86}	$\alpha^7+\alpha^5+\alpha^4+1$	10110001
α^{87}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha+1$	01111111
α^{88}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha$	11111110
α^{89}	$\alpha^7+\alpha^6+\alpha^5+1$	11100001
α^{90}	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha+1$	11011111
α^{91}	$\alpha^7+\alpha^5+\alpha+1$	10100011
α^{92}	$\alpha^6+\alpha^4+\alpha^3+\alpha+1$	01011011
α^{93}	$\alpha^7+\alpha^5+\alpha^4+\alpha^2+\alpha$	10110110
α^{94}	$\alpha^6+\alpha^5+\alpha^4+1$	01110001
α^{95}	$\alpha^7+\alpha^6+\alpha^5+\alpha$	11100010
α^{96}	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+1$	11011001
α^{97}	$\alpha^7+\alpha^5+\alpha^3+\alpha^2+\alpha+1$	10101111
α^{98}	$\alpha^6+\alpha+1$	01000011
α^{99}	$\alpha^7+\alpha^2+\alpha$	10000110
α^{100}	α^4+1	00010001
α^{101}	$\alpha^5+\alpha$	00100010
α^{102}	$\alpha^6+\alpha^2$	01000100
α^{103}	$\alpha^7+\alpha^3$	10001000
α^{104}	$\alpha^3+\alpha^2+1$	00001101
α^{105}	$\alpha^4+\alpha^3+\alpha$	00011010
α^{106}	$\alpha^5+\alpha^4+\alpha^2$	00110100
α^{107}	$\alpha^6+\alpha^5+\alpha^3$	01101000
α^{108}	$\alpha^7+\alpha^6+\alpha^4$	11010000
α^{109}	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$	10111101
α^{110}	$\alpha^6+\alpha^5+\alpha^2+\alpha+1$	01100111
α^{111}	$\alpha^7+\alpha^6+\alpha^3+\alpha^2+\alpha$	11001110

べき	展開	ベクトル
α^{112}	α^7+1	10000001
α^{113}	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$	00011111
α^{114}	$\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha$	00111110
α^{115}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2$	01111100
α^{116}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3$	11111000
α^{117}	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha^2+1$	11101101
α^{118}	$\alpha^7+\alpha^6+\alpha^2+\alpha+1$	11000111
α^{119}	$\alpha^7+\alpha^4+\alpha+1$	10010011
α^{120}	$\alpha^5+\alpha^4+\alpha^3+\alpha+1$	00111011
α^{121}	$\alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha$	01110110
α^{122}	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha^2$	11101100
α^{123}	$\alpha^7+\alpha^6+\alpha^2+1$	11000101
α^{124}	$\alpha^7+\alpha^4+\alpha^2+\alpha+1$	10010111
α^{125}	$\alpha^5+\alpha^4+\alpha+1$	00110011
α^{126}	$\alpha^6+\alpha^5+\alpha^2+\alpha$	01100110
α^{127}	$\alpha^7+\alpha^6+\alpha^3+\alpha^2$	11001100
α^{128}	$\alpha^7+\alpha^2+1$	10000101
α^{129}	$\alpha^4+\alpha^2+\alpha+1$	00010111
α^{130}	$\alpha^5+\alpha^3+\alpha^2+\alpha$	00101110
α^{131}	$\alpha^6+\alpha^4+\alpha^3+\alpha^2$	01011100
α^{132}	$\alpha^7+\alpha^5+\alpha^4+\alpha^3$	10111000
α^{133}	$\alpha^6+\alpha^5+\alpha^3+\alpha^2+1$	01101101
α^{134}	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha$	11011010
α^{135}	$\alpha^7+\alpha^5+\alpha^3+1$	10101001
α^{136}	$\alpha^6+\alpha^3+\alpha^2+\alpha+1$	01001111
α^{137}	$\alpha^7+\alpha^4+\alpha^3+\alpha^2+\alpha$	10011110
α^{138}	α^5+1	00100001
α^{139}	$\alpha^6+\alpha$	01000010
α^{140}	$\alpha^7+\alpha^2$	10000100
α^{141}	$\alpha^4+\alpha^2+1$	00010101
α^{142}	$\alpha^5+\alpha^3+\alpha$	00101010
α^{143}	$\alpha^6+\alpha^4+\alpha^2$	01010100
α^{144}	$\alpha^7+\alpha^5+\alpha^3$	10101000
α^{145}	$\alpha^6+\alpha^3+\alpha^2+1$	01001101
α^{146}	$\alpha^7+\alpha^4+\alpha^3+\alpha$	10011010
α^{147}	$\alpha^5+\alpha^3+1$	00101001
α^{148}	$\alpha^6+\alpha^4+\alpha$	01010010
α^{149}	$\alpha^7+\alpha^5+\alpha^2$	10100100
α^{150}	$\alpha^6+\alpha^4+\alpha^2+1$	01010101
α^{151}	$\alpha^7+\alpha^5+\alpha^3+\alpha$	10101010
α^{152}	$\alpha^6+\alpha^3+1$	01001001
α^{153}	$\alpha^7+\alpha^4+\alpha$	10010010
α^{154}	$\alpha^5+\alpha^4+\alpha^3+1$	00111001
α^{155}	$\alpha^6+\alpha^5+\alpha^4+\alpha$	01110010
α^{156}	$\alpha^7+\alpha^6+\alpha^5+\alpha^2$	11100100
α^{157}	$\alpha^7+\alpha^6+\alpha^4+\alpha^2+1$	11010101
α^{158}	$\alpha^7+\alpha^5+\alpha^4+\alpha^2+\alpha+1$	10110111
α^{159}	$\alpha^6+\alpha^5+\alpha^4+\alpha+1$	01110011

べき	展開	ベクトル
α^{160}	$\alpha^7+\alpha^6+\alpha^5+\alpha^2+\alpha$	11100110
α^{161}	$\alpha^7+\alpha^6+\alpha^4+1$	11010001
α^{162}	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha+1$	10111111
α^{163}	$\alpha^6+\alpha^5+\alpha+1$	01100011
α^{164}	$\alpha^7+\alpha^6+\alpha^2+\alpha$	11000110
α^{165}	$\alpha^7+\alpha^4+1$	10010001
α^{166}	$\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha+1$	00111111
α^{167}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha$	01111110
α^{168}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2$	11111100
α^{169}	$\alpha^7+\alpha^6+\alpha^5+\alpha^2+1$	11100101
α^{170}	$\alpha^7+\alpha^6+\alpha^4+\alpha^2+\alpha+1$	11010111
α^{171}	$\alpha^7+\alpha^5+\alpha^4+\alpha+1$	10110011
α^{172}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha+1$	01111011
α^{173}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha$	11110110
α^{174}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+1$	11110001
α^{175}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha+1$	11111111
α^{176}	$\alpha^7+\alpha^6+\alpha^5+\alpha+1$	11100011
α^{177}	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha+1$	11011011
α^{178}	$\alpha^7+\alpha^5+\alpha^3+\alpha+1$	10101011
α^{179}	$\alpha^6+\alpha^3+\alpha+1$	01001011
α^{180}	$\alpha^7+\alpha^4+\alpha^2+\alpha$	10010110
α^{181}	$\alpha^5+\alpha^4+1$	00110001
α^{182}	$\alpha^6+\alpha^5+\alpha$	01100010
α^{183}	$\alpha^7+\alpha^6+\alpha^2$	11000100
α^{184}	$\alpha^7+\alpha^4+\alpha^2+1$	10010101
α^{185}	$\alpha^5+\alpha^4+\alpha^2+\alpha+1$	00110111
α^{186}	$\alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha$	01101110
α^{187}	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2$	11011100
α^{188}	$\alpha^7+\alpha^5+\alpha^2+1$	10100101
α^{189}	$\alpha^6+\alpha^4+\alpha^2+\alpha+1$	01010111
α^{190}	$\alpha^7+\alpha^5+\alpha^3+\alpha^2+\alpha$	10101110
α^{191}	α^6+1	01000001
α^{192}	$\alpha^7+\alpha$	10000010
α^{193}	$\alpha^4+\alpha^3+1$	00011001
α^{194}	$\alpha^5+\alpha^4+\alpha$	00110010
α^{195}	$\alpha^6+\alpha^5+\alpha^2$	01100100
α^{196}	$\alpha^7+\alpha^6+\alpha^3$	11001000
α^{197}	$\alpha^7+\alpha^3+\alpha^2+1$	10001101
α^{198}	$\alpha^2+\alpha+1$	00000111
α^{199}	$\alpha^3+\alpha^2+\alpha$	00001110
α^{200}	$\alpha^4+\alpha^3+\alpha^2$	00011100
α^{201}	$\alpha^5+\alpha^4+\alpha^3$	00111000
α^{202}	$\alpha^6+\alpha^5+\alpha^4$	01110000
α^{203}	$\alpha^7+\alpha^6+\alpha^5$	11100000
α^{204}	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+1$	11011101
α^{205}	$\alpha^7+\alpha^5+\alpha^2+\alpha+1$	10100111
α^{206}	$\alpha^6+\alpha^4+\alpha+1$	01010011
α^{207}	$\alpha^7+\alpha^5+\alpha^2+\alpha$	10100110

べき	展開	ベクトル
α^{208}	$\alpha^6+\alpha^4+1$	01010001
α^{209}	$\alpha^7+\alpha^5+\alpha$	10100010
α^{210}	$\alpha^6+\alpha^4+\alpha^3+1$	01011001
α^{211}	$\alpha^7+\alpha^5+\alpha^4+\alpha$	10110010
α^{212}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+1$	01111001
α^{213}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha$	11110010
α^{214}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+1$	11111001
α^{215}	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha+1$	11101111
α^{216}	$\alpha^7+\alpha^6+\alpha+1$	11000011
α^{217}	$\alpha^7+\alpha^4+\alpha^3+\alpha+1$	10011011
α^{218}	$\alpha^5+\alpha^3+\alpha+1$	00101011
α^{219}	$\alpha^6+\alpha^4+\alpha^2+\alpha$	01010110
α^{220}	$\alpha^7+\alpha^5+\alpha^3+\alpha^2$	10101100
α^{221}	$\alpha^6+\alpha^2+1$	01000101
α^{222}	$\alpha^7+\alpha^3+\alpha$	10001010
α^{223}	α^3+1	00001001
α^{224}	$\alpha^4+\alpha$	00010010
α^{225}	$\alpha^5+\alpha^2$	00100100
α^{226}	$\alpha^6+\alpha^3$	01001000
α^{227}	$\alpha^7+\alpha^4$	10010000
α^{228}	$\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$	00111101
α^{229}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha$	01111010
α^{230}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2$	11110100
α^{231}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2+1$	11110101
α^{232}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha+1$	11110111
α^{233}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha+1$	11110011
α^{234}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha+1$	11111011
α^{235}	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha+1$	11101011
α^{236}	$\alpha^7+\alpha^6+\alpha^3+\alpha+1$	11001011
α^{237}	$\alpha^7+\alpha^3+\alpha+1$	10001011
α^{238}	$\alpha^3+\alpha+1$	00001011
α^{239}	$\alpha^4+\alpha^2+\alpha$	00010110
α^{240}	$\alpha^5+\alpha^3+\alpha^2$	00101100
α^{241}	$\alpha^6+\alpha^4+\alpha^3$	01011000
α^{242}	$\alpha^7+\alpha^5+\alpha^4$	10110000
α^{243}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$	01111101
α^{244}	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha$	11111010
α^{245}	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+1$	11101001
α^{246}	$\alpha^7+\alpha^6+\alpha^3+\alpha^2+\alpha+1$	11001111
α^{247}	$\alpha^7+\alpha+1$	10000011
α^{248}	$\alpha^4+\alpha^3+\alpha+1$	00011011
α^{249}	$\alpha^5+\alpha^4+\alpha^2+\alpha$	00110110
α^{250}	$\alpha^6+\alpha^5+\alpha^3+\alpha^2$	01101100
α^{251}	$\alpha^7+\alpha^6+\alpha^4+\alpha^3$	11011000
α^{252}	$\alpha^7+\alpha^5+\alpha^3+\alpha^2+1$	10101101
α^{253}	$\alpha^6+\alpha^2+\alpha+1$	01000111
α^{254}	$\alpha^7+\alpha^3+\alpha^2+\alpha$	10001110
0	0	00000000

A.2 ガロア拡大体 $\mathbf{GF}(2^4)$ のべき表現とベクトル表現

1. 原始多項式 (既約多項式) は x^4+x+1 とする ($\alpha^4=\alpha+1$)。
   なお、$\alpha^{2^4-1} \equiv \alpha^{15} \equiv \alpha^0 \equiv 1 \bmod (\alpha^4+\alpha+1)$ より、$\alpha^{15}=1$。
2. 多項式の係数は 2 を法とする (mod 2)。

べき表現	展開	ベクトル
α^0	1	0001
α^1	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	1100
α^7	$\alpha^3+\alpha+1$	1011
α^8	α^2+1	0101
α^9	$\alpha^3+\alpha$	1010
α^{10}	$\alpha^2+\alpha+1$	0111
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1101
α^{14}	α^3+1	1001
0	0	0000