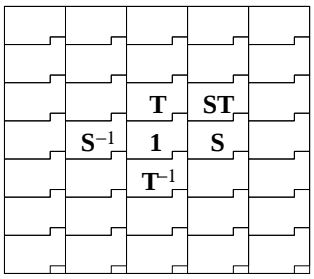
応用代数講義　ウェッブ付録A
教科書の補遺

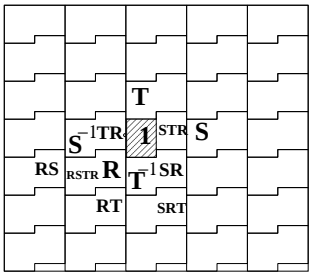
p.49, (図を除いて数えて) 上から **10** 行目　あみだくじの場合もそうですが，プログラミングと数学的な置換との対応は, 置換そのものより逆置換を用いるときれいになります．このため, 暗号などのプログラミングでは, 逆置換の作用を単に置換と呼ぶことも多いようです．サポートページのゲーム“ピラミンクス”の解でもこの対応法を使っていますので，詳細についてはそちらを参照してください．

p.60, 問 3.7 の解答の詳細版：まず図 3.6 の拡大版に記号を追加したものを掲げる．



ST=TS

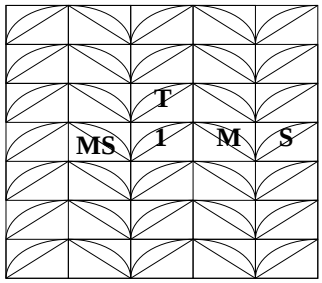
p1



TS=ST
R^2 =1
RSR=S^{-1}
RTR=T^{-1}

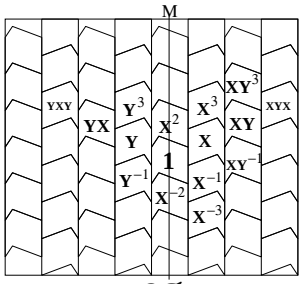
other rotations:
SR=P
TR=Q

p2



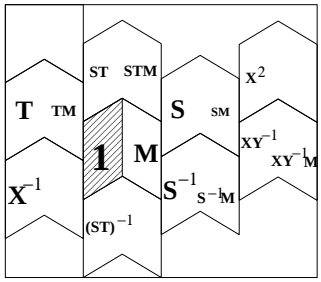
ST=TS
MT=TM
M^2 =1
MS^2 =1
or
MSM=S^{-1}

pm



X^2=Y^2

pg

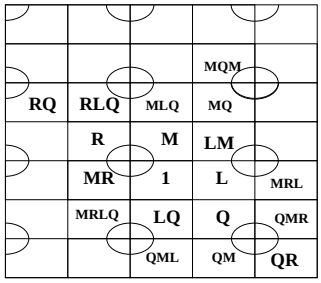


<X,M>

M^2=1

X=SM　S=XM
T=MX=MSM
Y=TM=MS=MXM

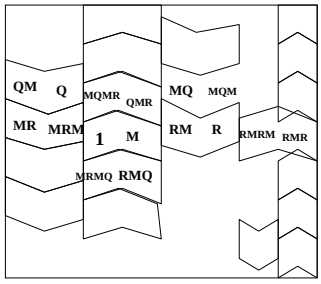
cm



LM=ML
LQ=QL
MR=RM
L^2 =M^2 =Q^2 =R^2=1
MR=RM

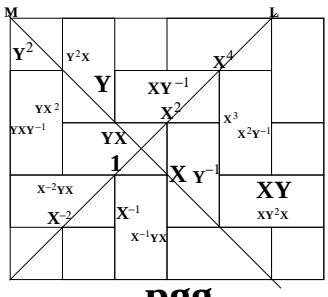
S=MRL
T=MLQ

pmm



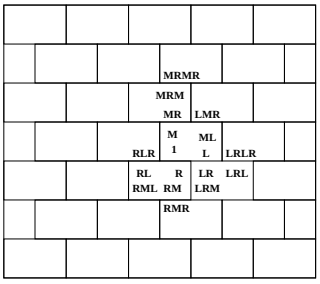
M^2 =Q^2=R^2=1
(MQ)^2=(RM)^2

pmg



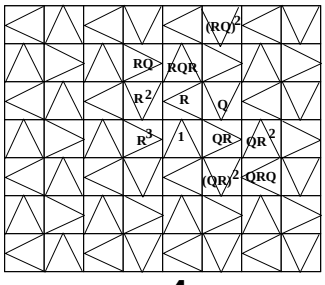
(YX)^2= 1
(XY^{-1})^2= 1

pgg



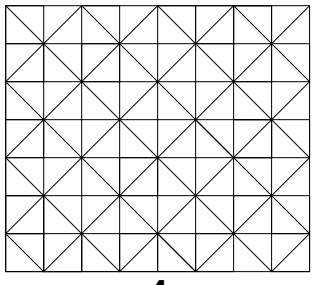
ML=LM
M^2=R^2=L^2=1

cmm

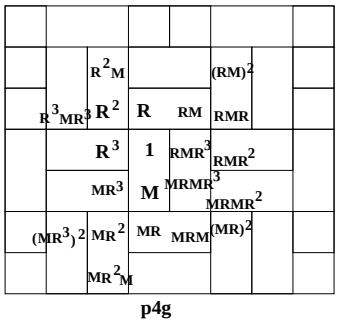


Q^2 = R^4 =1
(QR)^4 =1

p4



p4m



p4g

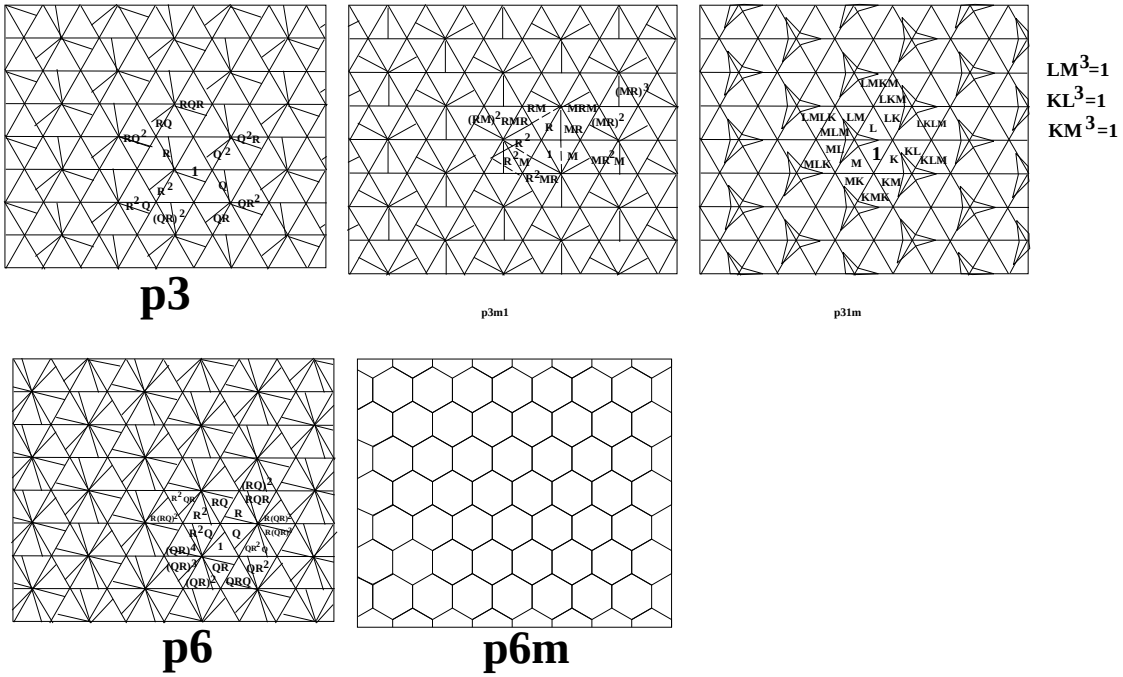


図 **3.6** 17 種の繰り返し模様 (ラベルは **X** 線結晶学の国際標準記号)

各パターンについて, 順に群の構造と 生成元を 示す. 以下，S, T は二つの1 次独立な平行移動を，K, L, M, N は異なる軸に関する鏡映を，P_θ, Q_θ, R_θ は異なる中心に関する角 θ の回転を 表す．また X, Y は並進鏡映 (鏡映と 平行移動を 組み合わせたもの) を 表す．紙数の関係で詳細な図は本書のサポート ヘージに回す.

p1: $\langle S, T\rangle$, 基本領域はパターン一つ分.

p2: $\langle S, T, R_\pi\rangle$, 基本関係は $R_\pi^2 = \mathrm{id}$, $R_\pi S R_\pi = S^{-1}$, $R_\pi T R_\pi = T^{-1}$. または，$\langle P_\pi, Q_\pi, R_\pi\rangle$, $S = PQ$, $T = RQ$ の関係にある．基本領域はパターンの左半分.

pm: $\langle S, T, M\rangle$, 基本関係は $ST = TS$, $TM = MT$, $M^2 = (MS)^2 = \mathrm{id}$ で，$L = MS$ が M に平行な軸を 持つ第2 の鏡映となる．あるいは $\langle L, M, T\rangle$ (二つの鏡映と 一つの平行移動), $S = ML$ が残り の平行移動に対応. 基本領域は長方形一つ分. なお，群構造は同じだが，鏡映の軸が 45° 傾いたパターンも 有る．

pg: $\langle X, Y\rangle$ (共通の対称軸を 持つ二つの並進鏡映: $X = SM$, $Y = TM$, ただし S, T, M 自身は含まれない), 基本関係は $X^2 = Y^2$. これと XY^{-1} が二つの平行移動を 与える．基本領域はパターン一つ分.

cm: pg に鏡映が加わったもの．$\langle S, T, M\rangle$. あるいは, $\langle X, M\rangle$ (一つの鏡映とそれを 軸とする 並進鏡映), ちなみに $S = XM$, $T = MX$ で, もう一つの並進鏡映は $Y = MXM$ で与えられる．基本領域はパターン一つの左半分.

pmm: $\langle K, L, M, N\rangle$ (長方形の4 辺に関する 鏡映). KM, LN が平行移動の基本ベクト ルを 成し，その他の組合せは可換．あるいは，$\langle L, M, Q_\pi, R_\pi\rangle$ (互いに垂直な軸に関する 二つの鏡映とそれぞれの軸上の点を 中心とする 二つの 180° 回転). L と M, L と Q, M と R はそれぞれ可換で，LQ, MR が残り 二つの鏡映となる．$S = MRL$, $T = MLQ$ が平行移動．基本領域は長方形一つ分.

pmg: $\langle M, Q_\pi, R_\pi\rangle$ (一つの鏡映とその軸上に無い2 点を 中心とする 二つの 180° 回転), 基本領域はパターンの左半分.

pgg: $\langle X, Y\rangle$ (二つの垂直な軸を 持つ並進鏡映), 関係式は $(YX)^2 = (XY^{-1})^2 = 1$ で, これらが 180° の回転を 与える．X^2 と Y^2 が可換な平行移動とな る．基本領域は長方形を 細長い方に切った半分.

cmm: $\langle L, M, R_\pi\rangle$ (二つの垂直な 鏡映と 一つの 180° 回転), 関係式は $LM = ML$, $L^2 = M^2 = R^2 = \mathrm{id}$. 基本領域は4 分の1 長方形.

p4: p4m から鏡映を除いたもの $\langle S, T, R_{\pi/2}\rangle$. あるいは $\langle Q_\pi, R_{\pi/2}\rangle$ (一つの 180° 回転と一つの 90° 回転), 関係式は $Q_\pi^2 = R_{\pi/2}^4 = \mathrm{id}$, $(Q_\pi R_{\pi/2})^4 = \mathrm{id}$. 平行移動は $S = QR^2$, $T = RQR$, 基本領域は正方形1 個分.
p4m: 平行移動と D_4 の合成. あるいは直角2 等辺3 角形の3 辺に関する鏡映. 基本領域は直角2 等辺3 角形1 個分.
p4g: $\langle R_\pi, M\rangle$ (一つの鏡映とその上に無い点を中心とする一つの 90° 回転), 基本領域は長方形の半分を成す正方形.
p3: p6 から鏡映を除いたもの. 二つの 120° 回転 Q, R
で生成される. もう一つの回転は (QR) で $(QR)^3 = \mathrm{id}$ が関係式. Q^2R と RQ^2 が独立な平行移動となる. 基本領域は正3 角形2 個が成す菱形.
p3m1: $\langle R_{2\pi/3}, M\rangle$ (一つの鏡映と一つの 120° 回転), 関係式は $M^2 = R_{2\pi/3}^3 = 1$. $(MR_{2\pi/3})^2$ と $(R_{2\pi/3}M)^2$ が独立な平行移動となる. 基本領域は正6 角形の頂点と中心を結ぶ線分を対称軸とする6 分の1 領域.
p31m: 平行移動と D_3 の合成 $\langle S, T, R_{2\pi/3}, M\rangle$, 基本関係は $R_{2\pi/3}^3 = M^2 = \mathrm{id}$, $R_{2\pi/3}S = SR_{2\pi/3}$, $R_{2\pi/3}M = MR_{2\pi/3}$. あるいは $\langle K, L, M\rangle$ (正3 角形の3 辺に関する鏡映), 基本関係は $K^2 = L^2 = M^2 = \mathrm{id}$, $(KL)^3 = (KM)^3 = (LM)^3 = \mathrm{id}$. ちなみに, $S = LKLM$, $T = LMLK$ が独立な平行移動. 基本領域は正3 角形1 個分.
p6: p6m から鏡映を除いたもの. 最小生成元としては, $\langle$
$Q_\pi, R_{2\pi/3}\rangle$ (一つの 180° 回転と一つの 120° 回転) が取れる. QR が -60° の回転, $S = R(QR)^2$, $T = R(RQ)^2$ が独立な平行移動となる. 基本領域は正3 角形一つ分.
p6m: 正6 角形の対称群 D_6 とその中心の平行移動より成る. これは, D_6 が正6 角形に作用するときの基本領域である 30°, 60° の直角3 角形の3 辺に関する鏡映 K, L, M でも生成される. 基本関係は $K^2 = L^2 = M^2 = \mathrm{id}$, $(KM)^2 = (ML)^3 = (KL)^6 = \mathrm{id}$. 基本領域は上述の直角3 角形1 個分.

著作権の関係で, あまり芸術的でない図を自分で描いたが, 教科書の参考文献に載せた Weyl や Coxeter の本, あるいはウェッブサイトには美しい模様が載っており, 実際にアルハンブラ宮殿の装飾模様なども手に入るので, サーチして見られるとよい.

p.210, 問 8.3 の解答の詳細版: 練習として, 手始めに $\boldsymbol{F}_{2^3}$ を $\boldsymbol{F}_2[x]/(x^3 + x + 1)$ として定義したときの演算の表を作ってみる.

加法

$\diagdown$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

乗法

$\diagdown$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

$\boldsymbol{F}_{2^4} = \boldsymbol{F}_2[x]/(x^4+x+1)$ の場合は, $c_3\alpha^3 + c_2\alpha_2 + c_1\alpha + c_0$ を $c_3c_2c_1c_0$ と略記すると,

加法

$\diagdown$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0001	0001	0000	0011	0010	0101	0100	0111	0110	1001	1000	1011	1010	1101	1100	1111	1110
0010	0010	0011	0000	0001	0110	0111	0100	0101	1010	1011	1000	1001	1110	1111	1100	1101
0011	0011	0010	0001	0000	0111	0110	0101	0100	1011	1010	1001	1000	1111	1110	1101	1100
0100	0100	0101	0110	0111	0000	0001	0010	0011	1100	1101	1110	1111	1000	1001	1010	1011
0101	0101	0100	0111	0110	0001	0000	0011	0010	1101	1100	1111	1110	1001	1000	1011	1010
0110	0110	0111	0100	0101	0001	0000	0011	0010	1101	1100	1111	1110	1001	1000	1011	1010
0111	01111	0110	0101	0100	0011	0010	0001	0000	1111	1110	1101	1100	1011	1010	1001	1000
1000	1000	1001	1010	1011	1100	1101	1110	1111	0000	0001	0010	0011	0100	0101	0110	0111
1001	1001	1000	1011	1010	1101	1100	1111	1110	0001	0000	0011	0010	0101	0100	0111	0119
1010	1010	1011	1000	1001	1110	1111	1100	1101	0010	0011	0000	0001	0110	0111	0100	0101
1011	1011	1010	1001	1000	1111	1110	1100	1100	0011	0010	0001	0000	0111	0110	0101	0100
1100	1100	1101	1110	0011	1000	1001	1010	1011	0100	0101	0110	0111	0100	0101	0110	0111
1101	1101	1100	1110	1111	1001	1000	1011	1010	0101	0100	0111	0110	0001	0000	0011	0010
1110	1110	1111	1100	1101	1010	1011	1000	1001	01110	0011	0100	0101	0010	0011	0000	0001
1111	1111	1110	1101	1100	1010	1010	1001	1000	0001	0110	0101	0100	0011	0010	0001	0000

乗法

＼	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
0001	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0010	0000	0010	0100	0110	1000	1010	1100	1110	0011	0001	0111	0101	1011	1001	1111	1101
0011	0000	0011	0110	0101	1100	1111	1010	1001	1011	1000	1101	1110	0111	0100	0001	0010
0100	0000	0100	1000	1100	0011	0111	1011	1111	0110	0010	1110	1010	0101	0001	1101	1001
0101	0000	0101	1010	1111	0111	0010	1101	1000	1110	1011	0100	0001	1001	1100	0011	0110
0110	0000	0110	1100	1010	1011	1101	0111	0001	0101	0011	1001	1111	1110	1000	0010	0100
0111	0000	0111	1110	1001	1111	1000	0001	0110	1101	1010	0011	0100	0010	0101	1100	1011
1000	0000	1000	0011	1011	0110	1110	0101	1101	1100	0100	1111	0111	1010	0010	1001	0001
1001	0000	1001	0001	1000	0010	1011	0011	1010	0100	1101	0101	1100	0110	1111	0111	1110
1010	0000	1010	0111	1101	1110	0100	1001	0011	1111	0101	1000	0010	0001	1011	0110	1100
1011	0000	1011	0101	1110	1010	0001	1111	0100	0111	1100	0010	1001	1101	0110	1000	0011
1100	0000	1100	1011	0111	0101	1001	1110	0010	1010	0110	0001	1101	1111	0011	0100	1000
1101	0000	1101	1001	0100	0001	1100	1000	0101	0010	1111	1011	0110	0011	1110	1010	0111
1110	0000	1110	1111	0001	1101	0011	0010	1100	1001	0111	0110	1000	0100	1010	1011	0101
1111	0000	1111	1101	0010	1001	0110	0100	1011	0001	1110	1100	0011	1000	0111	0101	1010

p.158, 上から 18 行目 $\mathrm{GCD}(k,n)=1$ のとき ζ に ζ^k を対応させると，これから $\forall j$ について $\zeta^j \mapsto \zeta^{jk}$ とならねばならないので，これが $L=K(\zeta)$ の体の同型に拡張できるとすれば一意ですが，L のすべての元の行き先が矛盾無く定まるかどうかは全く自明ではありません．もしこれが正しければ $\mathrm{Gal}(L/K)=\boldsymbol{Z}_n^*$ となると同時に，L/K の拡大次数は $\boldsymbol{Z}_n^*$ の位数 $\varphi(n)$ と等しくなりますが，このとき ζ の最小多項式は $\mathrm{GCD}(k,n)=1$ なるすべての k について ζ^k を根として持つことになります．逆に，これらの原始 n 乗根を根に持つ多項式 (円分多項式と呼びます) $\prod_{\mathrm{GCD}(k,n)=1}(x-\zeta^k)$ が既約なら，教科書の命題 7.13 により $\mathrm{Gal}(L/K)$ はこれらの根に推移的に作用し，従って $\mathrm{Gal}(L/K)=\boldsymbol{Z}_n^*$ となります．よって以下円分多項式が既約であることを証明します．

$n=p_1^{\nu_1}\cdots p_s^{\nu_s}$ を素因数分解とするとき，まず命題 4.25 ～ 4.27 により $|\boldsymbol{Z}_n^*|=p_1^{\nu_1-1}(p_1-1)\cdots p_s^{\nu_s-1}(p_s-1)$ であることを思い出しましょう．n が小さいときに実験してみると

n	$\lvert\boldsymbol{Z}_n^*\rvert$	$\boldsymbol{Z}_n^*$	$\Phi(n)$	x^n-1 の
2	1	(1)	x+1	$(x-1$
3	2	C_2	x^2+x+1	$(x-1$
4	2	C_2	x^2+1	$(x-1)(x$
5	4	C_4	$x^4+x^3+x^2+x+1$	$(x-1$
6	2	C_2	x^2+x+1	$(x-1)(x+1)($
7	6	C_6	$x^6+x^5+x^4+x^3+x^2+x+1$	$(x-1$
8	4	$C_2\times C_2$	x^4+1	$(x-1)(x+1$
9	6	C_6	x^6+x^3+1	$(x-1)(x^2+$
10	4	C_4	$x^4+x^3+x^2+x+1$	$(x-1)(x+1)(x^4-x$
11	10	C_{10}	$x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$	$(x-1$
12	4	$C_2\times C_2$	x^4-x^2+1	$(x-1)(x+1)(x^2+$
13	12	C_{12}	$x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$	$(x-1$
14	6	C_6	$x^6-x^5+x^4-x^3+x^2-x+1$	$(x-1)(x+1)(x^6+x^5+x$
15	8	$C_2\times C_4$	$x^8-x^7+x^5-x^4+x^3-x+1$	$(x-1)(x^2+x+1)(x^4-$

このような表は，Risa/Asir や Pari/GP を使えば即座に得られますが，手で計算するときの例として，$n=12$ の場合を見てみましょう．$\boldsymbol{Z}_{12}^*=\{1,5,7,11\}$ で，円分多項式は, $\zeta=e^{2\pi\sqrt{-1}/12}=e^{\pi\sqrt{-1}/6}$ として $(x-\zeta)(x-\zeta^5)(x-\zeta^7)(x-\zeta^{11})$ ですが，これを展開して有理係数を求めるよりは，逆に $x^{12}-1$ を次のように因数分解した方が速いのです．

$$x^{12}-1=(x^6-1)(x^6+1)=(x^6-1)(x^2+1)(x^4-x^2+1)$$

ここで，$\zeta^6=-1$ なので，因子 x^6-1 は ζ とは無関係なので，因数分解は略しました．(ただし ζ^2 はこの根となります.) 同様に，$x^2+1=0$ の根は $x^4=1$ を満たすので，これも ζ とは無関係です．(ただし ζ^3 はこの根となります．) これから x^4-x^2+1 が ζ の最小多項式であることが分ります．これは確かに $\boldsymbol{Z}_{12}^*$ の位数と同じ次数を持っています．

さて，証明ですが，まず $n=p$ が素数のときを調べます．ここでは，後ほど教科書の p.188 で簡単に紹介している代数的整数の概念が少し必要になります．代数的整数とは，モニックな（すなわち，最高次の係数が 1 の）整数係数多項式の根となるようなもののことで，“分母が不要な” という整数のニュアンスを代数的数に拡張したものです．以下では区別のため普通の整数 $\boldsymbol{Z}$ を有理数の整数という意味で “有理整数” と呼ぶことにします．ζ を 1 の原始 p 乗根とすれば，$\zeta_k=\zeta^k$, $k=1,2,\ldots,p-1$ はすべて原始根，すなわち $\boldsymbol{F}_p^\times$ の生成元となり，円分多項式は

$$\prod_{k=1}^{p-1}(x-\zeta_k)=x^{p-1}+\cdots+x+1$$

となります．よってこれが $\boldsymbol{Q}$ 上既約なことを言うのが目標ですが，初等的な議論だけではなかなか示せません．上の等式に $x=1$ を代入すると

$$\prod_{k=1}^{p-1}(1-\zeta_k)=p \tag{1}$$

が得られます．ζ_k はすべて原始根なので，任意の対 k,l について，$\zeta_l=\zeta_k^a$ となる $a\in\boldsymbol{N}$ が存在するので，

$$\frac{1-\zeta_l}{1-\zeta_k}=\frac{1-\zeta_k^a}{1-\zeta_k}=\zeta_k^{a-1}+\zeta_k^{a-2}+\cdots+\zeta_k+1$$

となります．ζ_k は定義により代数的整数なので，これらが環を成すことを認めれば，右辺は代数的整数となります．これは k,l を取り替えても成り立つので，この量はそれ自身もその逆数も代数的整数となるような元です．このような元は一般の環では可逆元あるいは単元と呼ばれますが，整数論では単数と呼ばれるのが普通です．次に，代数的数のノルムの概念を導入します．これは教科書では第 8 章の有限体の拡大の議論で使われていますが，一般のガロア拡大 L/K でも定義され，$\alpha\in L$ のノルム $N_{L/K}(\alpha)$ とは, α をガロア群 $\mathrm{Gal}(L/K)$ の元で写したものすべての積と定義します:

$$N_{L/K}(\alpha)=\prod_{\sigma\in\mathrm{Gal}(L/K)}\sigma(\alpha)$$

従って $\alpha\mapsto N_{L/K}(\alpha)$ は $L^\times\to K^\times$ の乗法的な写像となり，$\alpha\in K$ なら $N_{L/K}(\alpha)=\alpha^m$, ここに m はガロア群の位数，すなわち L/K の拡大次数，となります．

補題 1 $K=\boldsymbol{Q}$, $L=\boldsymbol{Q}(\zeta)$ のとき，L の単数のノルムは ±1 である．

証明 ノルムは一般に K の元，従って今の場合は有理数となるが，α が代数的整数なら，その共役も定義から明らかに代数的整数なので，代数的整数が環を成すことから，これらの積 $N_{L/K}(\alpha)$ も代数的整数となる．しかるに有理数が代数的整数なら，それは有理整数となる．これは次のような非常に初等的な事実から従う：

補題 2 有理整数係数のモニックな多項式に有理数の根が有れば，それは有理整数であり，かつそれは定数項の約数である．

この事実は受験数学でも使われるものなので，証明は各自試みられよ．さて，単数の場合は逆数にも同じことが言えるので，$N_{L/K}(\alpha)$ は有理整数の単元となり，従って ± 1 しか有り得ない． $\square$

すると，$1-\zeta_k =$ 単数 $\times (1-\zeta)$ とし，$\boldsymbol{Q}(\zeta)/\boldsymbol{Q}$ の実際の拡大次数, すなわち $\mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$ の位数を m として，(1) の両辺のノルムを取れば

$$\pm N_{L/K}(1-\zeta)^{p-1} = p^m$$

となり，ここで $m \leq p-1$ なので，これから $m = p-1, N(1-\zeta) = \pm p$ が従う．以上により $n = p$ が素数のときには証明できた．

次に $n = p^\nu$ が素数冪のときを調べます．ν に関する帰納法でもよいのですが，$\nu = 1$ の場合の上の論法がほぼ通用するので，いっぺんにやります．$\nu \geq 2$ とし，ζ を 1 の原始 p^ν 乗根とすれば，$\zeta^{p^{\nu-1}}$ は明らかに 1 の原始 p 乗根，従って既約多項式 $x^{p-1}+x^{p-2}+\cdots+x+1$ の根となります．よって ζ は $p^{\nu-1}(p-1)$ 次多項式

$$x^{p^{\nu-1}(p-1)} + x^{p^{\nu-1}(p-2)} + \cdots + x^{p^{\nu-1}} + 1$$

の根となりますが，$p^{\nu-1}(p-1)$ 個の原始根はすべてこの方程式を満たすので，$\zeta_k = \zeta^k$, $\mathrm{GCD}(k,n) = 1$ と置けば

$$\prod_{k:\mathrm{GCD}(k,n)=1} (x-\zeta_k) = x^{p^{\nu-1}(p-1)} + x^{p^{\nu-1}(p-2)} + \cdots + x^{p^{\nu-1}} + 1. \tag{2}$$

よって $x = 1$ として

$$\prod_{k:\mathrm{GCD}(k,n)=1} (1-\zeta_k) = p.$$

ここで $\boldsymbol{F}_{p^\nu}^\times$ も巡回群で，ζ_k はいずれもその生成元なので，先と同様，$\dfrac{1-\zeta_l}{1-\zeta_k}$ は単数となります．よって $1-\zeta_k =$ 単数 $\times (1-\zeta)$ と置き，$\boldsymbol{Q}(\zeta)/\boldsymbol{Q}$ の実際の拡大次数, すなわち $\mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$ の位数を m として，先と同様, 上の式の両辺のノルムを取れば

$$\pm N_{L/K}(1-\zeta)^{p^{\nu-1}(p-1)} = p^m$$

$m \leq p^{\nu-1}(p-1)$ なので，これから $m = p^{\nu-1}(p-1)$, かつ $N_{L/K}(1-\zeta) = \pm p$ が得られます．よってこの場合も証明されました．

最後に，一般の n については s に関する帰納法で示します．$s = 1$ のときはすなわち n が素数冪となるので，上に示した通りです．そこで $s \geq 2$ とし，$s-1$ まで成り立つとして，$n' = p_1^{\nu_1}\cdots p_{s-1}^{\nu_{s-1}}$ と置き，$p_s = p$, $\nu_s = \nu$ と略記すると，$n = n'p^\nu$ となります．また ζ を 1 の原始 n 乗根とすれば，$\eta = \zeta^{p^\nu}$ は明らかに 1 の原始 n' 乗根であり，帰納法の仮定により $K = \boldsymbol{Q}(\eta)$ は $\boldsymbol{Q}$ 上 $\varphi(n')$ 次のガロア拡大となっています．更に，$\xi = \zeta^{n'}$ は 1 の原始 p^ν 乗根となり，$K(\xi) = \boldsymbol{Q}(\zeta)$ が成り立ちます．実際，$\subset$ の向きは明らかですが，逆に $1 \leq \forall k \leq n-1 = n'p^\nu - 1$ について，$\mathrm{GCD}(n', p^\nu) = 1$ なので拡張ユークリッド互除法により $an' + bp^\nu = 1$ となる整数 a, b が存在するから，$\zeta^k = \zeta^{kan'}\zeta^{kbp^\nu} = \xi^{ka}\eta^{kb}$ は $K(\xi)$ に属します．よって (2) に対応する

$$\prod_{k:\mathrm{GCD}(k,p)=1} (x-\xi^k) = x^{p^{\nu-1}(p-1)} + x^{p^{\nu-1}(p-2)} + \cdots + x^{p^{\nu-1}} + 1$$

が K 上既約であることが言えれば，$\boldsymbol{Q}(\zeta)/\boldsymbol{Q}$ の拡大次数は $\varphi(n')p^{p^{\nu-1}(p-1)} = \varphi(n)$ となり，証明が完了します．上に $x = 1$ を代入すると

$$\prod_{k:\mathrm{GCD}(k,p)=1} (1-\xi^k) = p$$

$K = \boldsymbol{Q}(\eta)$, $L = K(\xi)$ としてこの両辺のノルム $N_{L/K}$ を取ると，先の議論と同様にして

$$CN_{L/K}(1-\xi)^{p^{\nu-1}(p-1)} = p^m$$

となります．ここで C は K の単元，m は L/K の実際の拡大次数です．更にこの両辺のノルム $N_{K/\boldsymbol{Q}}$ を取ると，

$$N_{K/\boldsymbol{Q}}(C)N_{K/\boldsymbol{Q}}(N_{L/K}(1-\xi)^{p^{\nu-1}(p-1)}) = \pm(N_{L/\boldsymbol{Q}}(1-\xi))^{p^{\nu-1}(p-1)}) = p^{mn'}$$

となります．よって有理整数 $N_{L/\boldsymbol{Q}}(1-\xi)$ は p 以外の素因子を持ち得ませんが，p は素数で $m \leq p^{\nu-1}(p-1)$, かつ $\mathrm{GCD}(n', p) = 1$ なので，これから $m = p^{\nu-1}(p-1)$, $N_{L/\boldsymbol{Q}}(1-\xi) = p^{n'}$ とならざるを得ません．

以上で証明が完了しましたが，K が $\boldsymbol{Q}$ 以外の体の場合には，ζ の円分多項式は必ずしも K 上既約とはならず，そのとき $\mathrm{Gal}(K(\zeta)/K)$ は $\boldsymbol{Z}_n^*$ の真部分群となります．例えば上の例の $n = 12$ のとき，$K = \boldsymbol{Q}(\sqrt{-1})$ とすると，

$$x^4 - x^2 + 1 = (x^2-1)^2 + x^2 = (x^2 + \sqrt{-1}x - 1)(x^2 - \sqrt{-1}x - 1)$$

と K 上因数分解され，ζ は因子 $x^2 - \sqrt{-1}x - 1$ の方の根であることが簡単に確かめられます:

$$\frac{\zeta^2 - 1}{\zeta} = \zeta - \frac{1}{\zeta} = 2\sqrt{-1}\sin\frac{\pi}{6} = \sqrt{-1}$$

同様の計算から，ζ^5 もこの方程式を満たすことが分るので，$\mathrm{Gal}(L/K)$ はこの場合, 単位元と $\zeta \mapsto \zeta^5$ という対応から定まる同型写像より成る $\boldsymbol{Z}_{12}^*$ の部分群 $\{1, 5\} \simeq C_2$ と同型になります．このとき $\zeta \mapsto \zeta^7$ という対応は L/K の自己同型に拡張できないことを念のため確認しておきましょう．$\zeta^7 = \zeta \cdot \zeta^6 = -\zeta$ に注意すると，

$$\sqrt{-1} = \frac{\zeta^2 - 1}{\zeta} \mapsto -\frac{\zeta^2 - 1}{\zeta} = -\sqrt{-1}$$

です．すなわち，この対応は L の自己同型には拡張できるかもしれませんが，K の元 $\sqrt{-1}$ を動かしてしまうので，$\mathrm{Gal}(L/K)$ の元にはなっていません．

p.220, 上から 20∼21 行目 $\boldsymbol{R}$ と $\boldsymbol{C}$ は実数体 $\boldsymbol{R}$ 上の線型空間としては次元が異なるので同型ではないが，有理数体 $\boldsymbol{Q}$ ではいずれも連続の濃度の代数的次元で同型となってしまう．従ってもちろん加法群としても同型である．$\boldsymbol{R}$ の．$\boldsymbol{Q}$-線形空間としての基底は Hamel 基底と呼ばれる．[16], 例題 10.5 にその構成法が与えられている．今この一つを Σ とすれば，$\boldsymbol{C}$ の基底は非連結和集合 $\Sigma \cup \Sigma$ で与えられる．ここではむしろ，$\Sigma + i\Sigma$ と書く方が分かりやすいであろう．無限集合論の一般論により，両者は 1 対 1 対応を持つ．これから有限次元のときと同様，$\boldsymbol{R}$ と $\boldsymbol{C}$ の $\boldsymbol{Q}$-線形空間としての同型写像が導かれる．$\boldsymbol{Q}$ の元による乗法を忘れれば，これは加法群としての同型となる．この同型を通して，$\boldsymbol{R}^+$ も $\boldsymbol{C}$ と群として同型になる．以上に挙げた以外には同型関係が無いことは, 可換性, $x^n = e$ の解の個数, 集合としての濃度などを手掛りに判断できる．

p.229, 問 3.10 (2) の解答への補足 ちょっと数が多いので初等的に求めようとすると数え落とす恐れがあるが，S_4 の元により多項式 $x_1x_2 + x_3x_4$ が移る先は，もとのものと $x_1x_3 + x_2x_4$, $x_1x_4 + x_2x_3$ の計3 個で，それぞれがこの多項式の固定部分群の剰余類に相当しているので，固定群の位数は S_4 の位数 24 を 3 で割った 8 となるはずである．