第 12 週

符号理論によってある程度データを正しく受信できる技術を学んだら，今度はそのデータを解析することを考えて見ましょう。以後はフーリエ解析の話です。

１．フーリエ級数の復習

関数 $f(t)$ をフーリエ級数で展開するとは，

$$f(t)=\frac{a_0}{2}+\sum_{k=1}^{\infty}a_k\cos\omega_0 kt+\sum_{k=1}^{\infty}b_k\sin\omega_0 kt$$

または，複素数まで拡大して，

$$f(t)=\sum_{k=1}^{\infty}C_k e^{i\omega_0 kt}$$

ということでした。ここで，ω_0 は T を $f(t)$ の周期とたとき $\omega_0=2\pi/T$ で，$i=\sqrt{-1}$ を意味します。数学で問題となることは，どんな $f(t)$ もこのような形に展開できるのか？ということですが，工学で扱うたいていの関数はこのように展開できるので，以後このことにはふれないようにします。また下の形でフーリエ級数に展開したときを**複素フーリエ展開**といいます。以下複素フーリエ展開を扱っていきます。

複素フーリエ展開したとき，C_k はどのようなものになるのかというと，C_k は $f(t)$ と $e^{i\omega_0 kt}$ との（規格化した）**内積** $\left\langle f(t),e^{i\omega_0 kt}\right\rangle$ です。ベクトル空間の内積は知っていても，関数 $f(t)$ と $g(t)$ の内積とは？。それは次のように定義されます。

$$\left\langle f(t),g(t)\right\rangle=\frac{1}{T}\int_{-T/2}^{T/2}f(t)g(t)dt$$

普通の数ベクトル空間で知っているように，内積は２つのベクトルの間の角度（$\cos\theta$）を与えます。これを応用して，もし $\left\langle f(t),g(t)\right\rangle=0$ なら２つの関数（ベクトル）は直角に交わっていると考えます。もし $\left\langle f(t),g(t)\right\rangle=1$ ならば２つの関数（ベクトル）は同方向を向いていて，もし $\left\langle f(t),g(t)\right\rangle=-1$ ならば２つの関数（ベクトル）は逆方向を向いていると考えるのです。このようなことから，内積 $\left\langle f(t),g(t)\right\rangle$ は２つの関数の相関を表しているのです。特に $g(t)=e^{i\omega_0 kt}$ のとき，すなわち，

$$\left\langle f(t),e^{i\omega_0 kt}\right\rangle=\frac{1}{T}\int_{-T/2}^{T/2}f(t)e^{i\omega_0 kt}dt$$

を関数 $f(t)$ の**フーリエ変換**といっています。

$f(t)$ のフーリエ変換 C_k は，複素数として出てきますが，それを $C_k=A_k+iB_k$ とおいて，A_k を実部スペクトル，B_k を虚部スペクトル，$\angle C=\tan^{-1}\dfrac{b_k}{a_k}$ を位相スペクトル，$|C_k|=\sqrt{{a_k}^2+{b_k}^2}$ を**振幅スペクトル**，$|C_k|^2$ を**パワースペクトル**といいます。　音波や電波などを受信したときに，それがどのような波であるのかを解析するときに，このようなスペクトルを計算し，グラフ化し，そして分析するのです。このような解析方法を**スペクトル解析（またはフーリエ解析）**といいます。

【練習１４】　　$f(t)$ が $\cos t$，　$\cos 2t$，　$\cos t+\cos 2t$ のフーリエ変換 C_k をそれぞれ求め，さらに，実部スペクトル，虚部スペクトル，位相スペクトル，振幅スペクトル，パワースペクトルを求めよ．

２．ＤＥＦ

我々はある電波をデジタルデータで受け取ったとします。そしてその波形をスペクトル解析することを考えます。デジタルデータであるため，電波を関数として考えるとそれは，連続的ではなく離散的に入ってきます。そのため離散的なフーリエ変換，すなわち**離散フーリエ変換**（Discrete Fourier Transform，略して **DFT**）を行わなければなりません。

今，送信間隔をΔtとして，N個のサンプルデータを受信したとしましょう。それを，

$$\{f_0, f_1, f_2, \cdots, f_{N-1}\}$$

とします。そして，

$$\mathbf{f} = (f_0, f_1, f_2, \cdots, f_{N-1}),\quad \mathbf{e}_k = (1, e^{ik\Delta\omega}, e^{i2k\Delta\omega}, e^{i3k\Delta\omega}, \cdots, e^{i(N-1)k\Delta\omega})$$

として，複素数ベクトルとしての（規格化した）内積$C_k = \langle \mathbf{f}, \mathbf{e}_k \rangle$を考えます。ここで，$\Delta\omega = \dfrac{2\pi}{N}$です。$C_k$を$\mathbf{f}$の離散フーリエ変換といいます。$C_k$を別な表現で書けば，

$$C_k = \frac{1}{N}\sum_{j=0}^{N-1} f_j e^{-i(2\pi/N)kj}$$

となります。

３．ＤＦＴの性質

命題１２.１（スペクトルの周期性）

$C_{k+N} = C_k$が成立する。

証明　$C_{k+N} = \dfrac{1}{N}\displaystyle\sum_{j=0}^{N-1} f_j e^{-i(2\pi/N)(k+N)j} = \dfrac{1}{N}\displaystyle\sum_{j=0}^{N-1} f_j e^{-i(2\pi/N)kj} e^{-i2\pi j}$

であり，jは整数なので，$e^{-i2\pi j}=1$。したがって証明された。$\square$

命題１２.２（スペクトルの対称性）

$C_{N-k} = C_{-k}$が成立する。

証明　$C_{N-k} = \dfrac{1}{N}\displaystyle\sum_{j=0}^{N-1} f_j e^{-i(2\pi/N)(N-k)j} = \dfrac{1}{N}\displaystyle\sum_{j=0}^{N-1} f_j e^{i(2\pi/N)kj} e^{-i2\pi j} = C_{-k}$　$\square$

第 13 週

2^n 点ＦＦＴ

　基本的には離散的なデータのスペクトル解析はＤＦＴで行うのですが，これをそのままコンピュータで計算させる方法は時間がかかりすぎて，実用的ではありません。そこで，高速フーリエ変換（Fast Fourier Transform，略して **FFT**）を利用することになります。ＦＦＴは普通 2^n にデータ数をとって行います。

$$\mathbf{f} = (f_0, f_1, f_2, \cdots, f_{N-1}),\quad \mathbf{e}_k = (1, e^{ik\Delta\omega}, e^{i2k\Delta\omega}, e^{i3k\Delta\omega}, \cdots, e^{i(N-1)k\Delta\omega})$$

として，$\mathbf{f}$ の離散フーリエ変換 C_k は,

$$C_k = \frac{1}{N}\sum_{j=0}^{N-1} f_j e^{-i(2\pi/N)kj}$$

でした。

１．4 点ＦＦＴ

　まずデータ数が $N=4$ の場合から考察していきます。以下 $e^{-i(2\pi/N)}$ を W と書くようにします。今 $N=4$ なので， $j \equiv k \bmod 4$ ならば，$W^j = W^k$ であることに注意します。すると，

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} W^0 & W^0 & W^0 & W^0 \\ W^0 & W^1 & W^2 & W^3 \\ W^0 & W^2 & W^0 & W^2 \\ W^0 & W^3 & W^2 & W^1 \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{pmatrix}$$

となります。これを計算すれば，W^j の計算が４回，掛け算が１６回，足し算が１２回で合計３２回の演算回数となります。この回数を減らす工夫を考えます。行列

$$A = \begin{pmatrix} W^0 & W^0 & W^0 & W^0 \\ W^0 & W^1 & W^2 & W^3 \\ W^0 & W^2 & W^0 & W^2 \\ W^0 & W^3 & W^2 & W^1 \end{pmatrix}$$

は $A = {}^tA$，すなわち対称行列になっています。法則性があるため演算の順序いれかえると次のようになります。

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} W^0 & W^0 & W^0 & W^0 \\ W^0 & W^2 & W^1 & W^3 \\ W^0 & W^0 & W^2 & W^2 \\ W^0 & W^2 & W^3 & W^1 \end{pmatrix} \begin{pmatrix} f_0 \\ f_2 \\ f_1 \\ f_3 \end{pmatrix}$$

このとき，行列 A は，次のようになります。

$$A' = \begin{pmatrix} W^0 & W^0 & W^0 & W^0 \\ W^0 & W^2 & W^1 & W^3 \\ W^0 & W^0 & W^2 & W^2 \\ W^0 & W^2 & W^3 & W^1 \end{pmatrix}$$

これを４等分してみると,

$$e = \begin{pmatrix} W^0 & W^0 \\ W^0 & W^2 \end{pmatrix},\quad B_1 = \begin{pmatrix} W^0 & W^0 \\ W^1 & W^3 \end{pmatrix},\quad B_2 = \begin{pmatrix} W^2 & W^2 \\ W^3 & W^1 \end{pmatrix},\quad A' = \begin{pmatrix} e & B_1 \\ e & B_2 \end{pmatrix},$$

となっています。ここで新しい行列演算を定義します。

$$\begin{bmatrix} x \\ y \end{bmatrix}\cdot\begin{pmatrix} a & b \\ c & d \end{pmatrix} \overset{def}{=} \begin{pmatrix} ax & bx \\ cy & dy \end{pmatrix}, \qquad \alpha\begin{bmatrix} x \\ y \end{bmatrix} \overset{def}{=} \begin{bmatrix} \alpha x \\ \alpha y \end{bmatrix}$$

この記号を使い，$W^{i+j}=W^iW^j$，$W^0=-W^2$，$W^1=-W^3$ であることに注意すると，

$$W_{B_1}=\begin{pmatrix} W^0 & W^0 \\ W^1 & W^3 \end{pmatrix}=\begin{bmatrix} W^0 \\ W^1 \end{bmatrix}\bullet\begin{pmatrix} W^0 & W^0 \\ W^0 & W^2 \end{pmatrix},$$

$$W_{B_2}=\begin{pmatrix} W^2 & W^2 \\ W^3 & W^1 \end{pmatrix}=\begin{bmatrix} W^2 \\ W^3 \end{bmatrix}\bullet\begin{pmatrix} W^0 & W^0 \\ W^0 & W^2 \end{pmatrix}=\begin{bmatrix} W^2 \\ W^2 \end{bmatrix}\bullet\left(\begin{bmatrix} W^0 \\ W^1 \end{bmatrix}\bullet\begin{pmatrix} W^0 & W^0 \\ W^0 & W^2 \end{pmatrix}\right)$$

であることがわかります。

以上のことから，４点の場合の基本要素は，

$$W_e=\begin{pmatrix} W^0 & W^0 \\ W^0 & W^2 \end{pmatrix}$$

です。さらにＦＦＴの計算を推し進めると，まず

$$W_{B_1}=\begin{bmatrix} W^0 \\ W^1 \end{bmatrix}\bullet W_e$$

の計算します。$W^2=-W^0$ に注意すると，ここでは，W^0, W^1 の計算で２回，掛け算が４回です。

次に

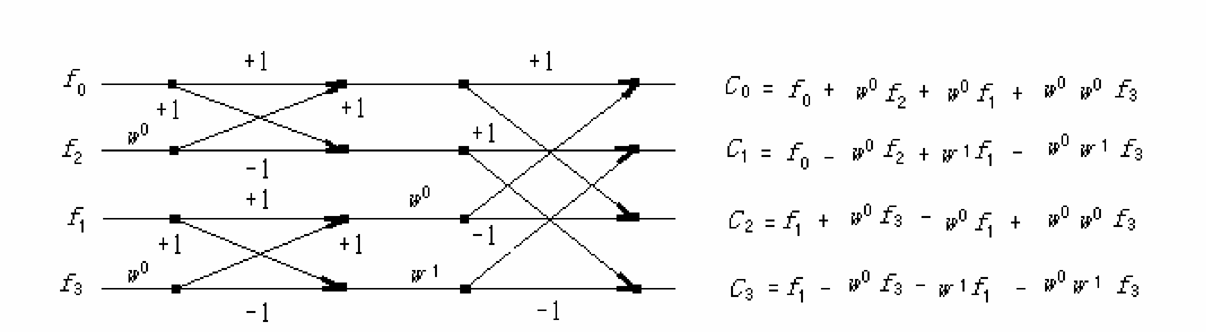
$$D_0=W_e\begin{pmatrix} f_0 \\ f_2 \end{pmatrix}, \qquad D_1=W_{B_1}\begin{pmatrix} f_1 \\ f_3 \end{pmatrix}$$

を計算します。ここでは，掛け算が８回，足し算が４回です。やはり $W^2=-W^0$ に注意すると，最後に

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix}=\begin{pmatrix} D_0+D_1 \\ D_0-D_1 \end{pmatrix}\begin{pmatrix} f_0 \\ f_2 \\ f_1 \\ f_3 \end{pmatrix}$$

を計算すればよく，ここでは，足し算が２回です。したがって演算回数の総合計は１６回となり演算回数は減少します。

上の演算を図式化すると次のように考えることもできます。



図の様子からこの演算方法を**バタフライ演算**と呼んでいます。

【練習１５】$f(t)=\cos t+\cos 2t$ を上記の方法により，$f(t)$ の離散フーリエ係数 C_0，C_2，C_3，

C_4 を求めよ。

さてデータ数４の場合において，計算のポイントは，$e,\ B_1$ でした。これらはそれぞれ $\begin{pmatrix} f_0 \\ f_2 \end{pmatrix},\ \begin{pmatrix} f_1 \\ f_3 \end{pmatrix}$ に作用します。つまり行列 $e,\ B_1$ はそれぞれ，$I_2=\{0,2\}$，$I_2+1=\{1,3\}$ に対応しています。さらに

$$W_{e_1}=\begin{pmatrix} W_e & W_{B_1} \\ W_e & [W^2]\bullet W_{B_1} \end{pmatrix}$$

とおくと，W_{e_1} は $I_1=\{0,2,1,3\}$ に対応します。ここで，$\left[W^2\right]=\begin{bmatrix} W^2 \\ W^2 \end{bmatrix}$ です。さらに，$\begin{bmatrix} W^2 \\ W^2 \end{bmatrix}\bullet W_{B_1}=-W_{B_1}$ となることに注意すると，

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix}=W_{e_1}\begin{pmatrix} f_0 \\ f_2 \\ f_1 \\ f_3 \end{pmatrix}$$

となります。行列 W を４点 FFT といいます。

２．８点ＦＦＴ

次にデータ数８場合を考察してみます。ここで扱う行列も対称行列です。今 $N=8$ なので，$j\equiv k \bmod 8$ ならば，$W^j=W^k$ であることに注意し，f について偶数と奇数に分けてみます。

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5 \\ C_6 \\ C_7 \end{pmatrix}=\begin{pmatrix} W^0 & W^0 & W^0 & W^0 \\ W^0 & W^2 & W^4 & W^6 \\ W^0 & W^4 & W^0 & W^4 \\ W^0 & W^6 & W^4 & W^2 \\ W^0 & W^0 & W^0 & W^0 \\ W^0 & W^2 & W^4 & W^6 \\ W^0 & W^4 & W^0 & W^4 \\ W^0 & W^6 & W^4 & W^2 \end{pmatrix}\begin{pmatrix} f_0 \\ f_2 \\ f_4 \\ f_6 \end{pmatrix}+\begin{bmatrix} \omega^0 \\ \omega^1 \\ \omega^2 \\ \omega^3 \\ -\omega^0 \\ -\omega^1 \\ -\omega^2 \\ -\omega^3 \end{bmatrix}\begin{pmatrix} W^0 & W^0 & W^0 & W^0 \\ W^0 & W^2 & W^4 & W^6 \\ W^0 & W^4 & W^0 & W^4 \\ W^0 & W^6 & W^4 & W^2 \\ W^0 & W^0 & W^0 & W^0 \\ W^0 & W^2 & W^4 & W^6 \\ W^0 & W^4 & W^0 & W^4 \\ W^0 & W^6 & W^4 & W^2 \end{pmatrix}\begin{pmatrix} f_1 \\ f_3 \\ f_5 \\ f_7 \end{pmatrix}$$

さらに，次のように変形します。

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5 \\ C_6 \\ C_7 \end{pmatrix} = \begin{pmatrix} W^0 & W^0 & W^0 & W^0 \\ W^0 & W^4 & W^2 & W^6 \\ W^0 & W^0 & W^4 & W^4 \\ W^0 & W^4 & W^6 & W^2 \\ W^0 & W^0 & W^0 & W^0 \\ W^0 & W^4 & W^2 & W^6 \\ W^0 & W^0 & W^4 & W^4 \\ W^0 & W^4 & W^6 & W^2 \end{pmatrix} \begin{pmatrix} f_0 \\ f_4 \\ f_2 \\ f_6 \end{pmatrix} + \begin{bmatrix} \omega^0 \\ \omega^1 \\ \omega^2 \\ \omega^3 \\ -\omega^0 \\ -\omega^1 \\ -\omega^2 \\ -\omega^3 \end{bmatrix} \begin{pmatrix} W^0 & W^0 & W^0 & W^0 \\ W^0 & W^4 & W^2 & W^6 \\ W^0 & W^0 & W^4 & W^4 \\ W^0 & W^4 & W^6 & W^2 \\ W^0 & W^0 & W^0 & W^0 \\ W^0 & W^4 & W^2 & W^6 \\ W^0 & W^0 & W^4 & W^4 \\ W^0 & W^4 & W^6 & W^2 \end{pmatrix} \begin{pmatrix} f_1 \\ f_5 \\ f_3 \\ f_7 \end{pmatrix}$$

先ほどと同じように分解して考えると，次が基本的であることがわかります。

$$W_e = \begin{pmatrix} W^0 & W^0 \\ W^0 & W^4 \end{pmatrix},\quad W_{B_1} = \begin{bmatrix} W^0 \\ W^2 \end{bmatrix} \bullet W_e,\quad \begin{pmatrix} W^4 & W^4 \\ W^6 & W^2 \end{pmatrix} = -\begin{bmatrix} W^0 \\ W^2 \end{bmatrix} \bullet W_e = -W_{B_1},$$

$$W_{e_1} = \begin{pmatrix} W_e & W_{B_1} \\ W_e & -W_{B_1} \end{pmatrix},\qquad W_{B_2} = \begin{bmatrix} W^0 \\ W^1 \\ W^2 \\ W^3 \end{bmatrix} \bullet W_{e_1}$$

ここで，$W^4 = -W^0$，$W^6 = -W^2$ を使っています。
以上より，

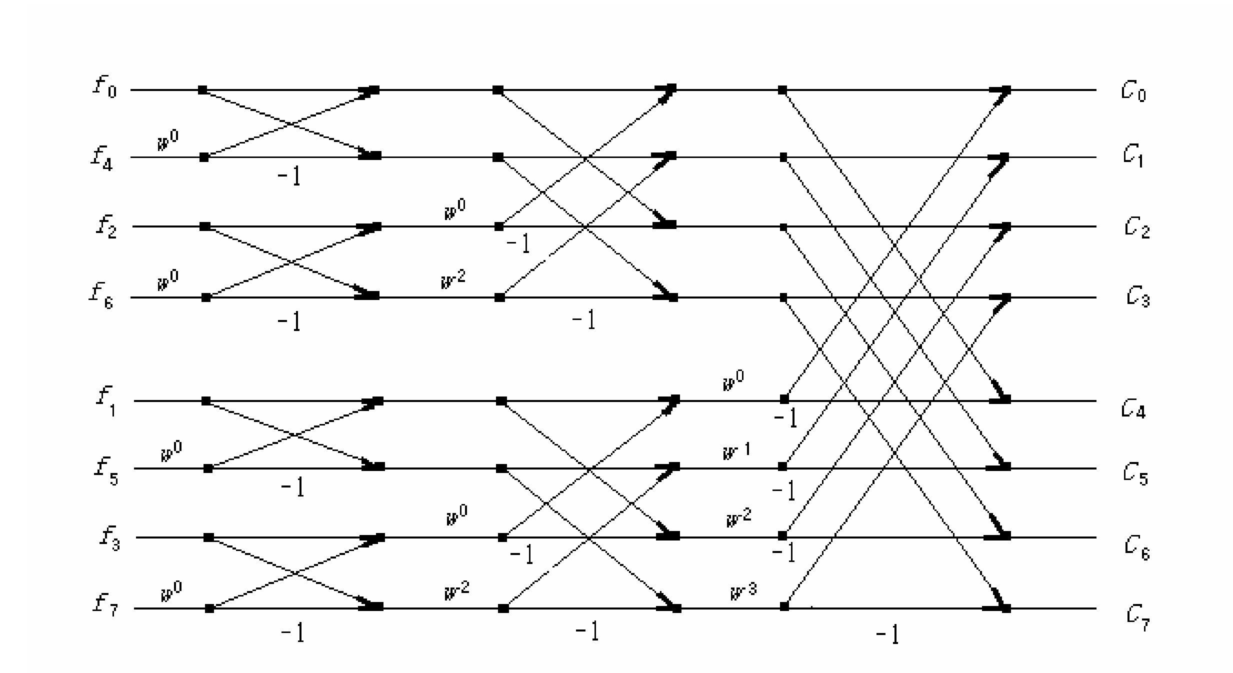
$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5 \\ C_6 \\ C_7 \end{pmatrix} = \begin{pmatrix} W_{e_1} \begin{pmatrix} f_0 \\ f_4 \\ f_2 \\ f_6 \end{pmatrix} + W_{B_2} \begin{pmatrix} f_1 \\ f_5 \\ f_3 \\ f_7 \end{pmatrix} \\ W_{e_1} \begin{pmatrix} f_0 \\ f_4 \\ f_2 \\ f_6 \end{pmatrix} - W_{B_2} \begin{pmatrix} f_1 \\ f_5 \\ f_3 \\ f_7 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{matrix} W_e \begin{pmatrix} f_0 \\ f_4 \end{pmatrix} + W_{B_1} \begin{pmatrix} f_2 \\ f_6 \end{pmatrix} \\ W_e \begin{pmatrix} f_0 \\ f_4 \end{pmatrix} - W_{B_1} \begin{pmatrix} f_2 \\ f_6 \end{pmatrix} \end{matrix} + W_{B_2} \begin{pmatrix} f_1 \\ f_5 \\ f_3 \\ f_7 \end{pmatrix} \\ \begin{matrix} W_e \begin{pmatrix} f_0 \\ f_4 \end{pmatrix} + W_{B_1} \begin{pmatrix} f_2 \\ f_6 \end{pmatrix} \\ W_e \begin{pmatrix} f_0 \\ f_4 \end{pmatrix} - W_{B_1} \begin{pmatrix} f_2 \\ f_6 \end{pmatrix} \end{matrix} - W_{B_2} \begin{pmatrix} f_1 \\ f_5 \\ f_3 \\ f_7 \end{pmatrix} \end{pmatrix}$$

を得ます。演算回数は自分で計算して見てください。相当数減少しているはずです。

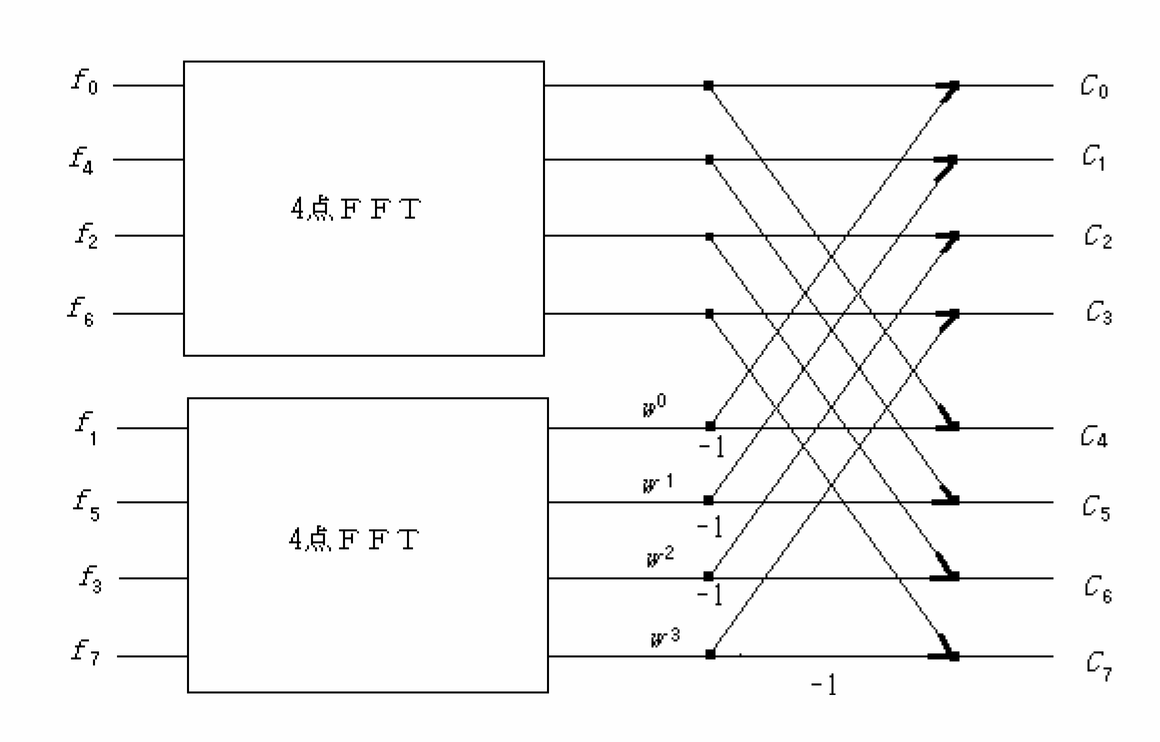
またの $I_4 = \{0,4\}$ に対応する行列は W_e で，　$I_4 + 2$ に対応する行列は W_{B_1} です。

さらに，　$I_2 = \{I_4, I_4 + 2\} = \{0,4,2,6\}$ には，行列 W_{e_1} が，$I_2 + 1 = \{1,5,3,7\}$ には行列 W_{B_2} が，$I_1 = \{I_2, I_2 + 1\} = \{0,4,2,6,1,5,3,7\}$ には行列 W_{e_2} がそれぞれ対応します。最後の e_2 から作られる行列 $W_{e_2} = \begin{pmatrix} W_{e_1} & W_{B_2} \\ W_{e_1} & -W_{B_2} \end{pmatrix}$ を **8 点 FFT** といいます。

8 点ＦＦＴの様子を前と同じように図示しますと，次のようになります。



上の図は 4 点ＦＦＴを利用して拡張されたものと考えることができます。それを分かりやすくかくと次の図になります。



この様子から 16 点ＦＦＴは 8 点ＦＦＴから拡張され, その図がどうなるかもすぐ分かると思います。

問題は図の左端に並べた f の添え字番号がどのような規則で並んでいるかです。これはビットリバーサル（bit reversal）というしくみで並べ替えられています。それは次回に詳しく述べます。

【課題１０】 $f(t)=\cos t+\cos 2t+\cos 3t$ を 8 点 FFT を用いて，離散フーリエ係数 $C_0,\cdots,C_7$ を求めよ。

第 14 週，第 15 週

１．ビットリバーサル

4 点ＦＦＴから考えていきます。4 点ＦＦＴのときの，添え字の並びは$0,1,2,3$でした。これを２進法，２ビットで考えます。

$$0 \leftrightarrow 00, \quad 1 \leftrightarrow 01, \quad 2 \leftrightarrow 10, \quad 3 \leftrightarrow 11$$

これをみてわかるように，１と２は 2 進でビットが入れ替わっているのです。

次に 8 進ＦＦＴで考えて見ます。同様に添え字の番号を 2 進法，3 ビットで考えみます。

$$0 \leftrightarrow 000, \quad 1 \leftrightarrow 001, \quad 2 \leftrightarrow 010, \quad 3 \leftrightarrow 011,$$

$$4 \leftrightarrow 100, \quad 5 \leftrightarrow 101, \quad 6 \leftrightarrow 110, \quad 7 \leftrightarrow 111$$

ビットの入れ替えが可能なのは，１と４，３と６で，実際に f の添え字は，$0,4,2,6,1,5,3,7$ となっています。

これは，2^n 点ＦＦＴに関してはいつもいえることで，ＦＦＴを行うにはまず，ビットリバーサルを行ってから始めなくてはいけないということになります。

２．ＦＦＴの数理

環の定義

定義１４.１　集合 R が**環**（ring）であるとは，次の条件（１），（２），（３）を満たすときをいう。

（１）　加法に関して可換群である。

（２）　乗法に関して半群である。

（３）　分配法則が成り立つ。

次に環 R の部分集合の中で特に重要な役割を果たすイデアルを定義します。

定義１４.２　環 R の部分集合 I がイデアルであるとは，次の条件（１），（２）を満たすときをいう。

（１）　任意の $a,b \in I$ に対し，$a+b \in I, -a \in I$

（２）　任意の $x \in R,\ a \in I$ に対し，$xa \in I$

以下簡単のために，環 R が積について単位元をもち，さらに可換であるとします。

定義１４.３　環 R のイデアル I は以下であるとする。

$$I = \{x_1 a_1 + \cdots + x_n a_n + z_1 a_1 + \cdots + z_n a_n : x_1, \cdots x_n \in R,\ z_1, \cdots, z_n \in \mathbb{Z}\}$$

このとき I は $a_1, \cdots, a_n$ で**生成される**イデアルといい，$I = (a_1, \cdots, a_n)$ と書く。

定義１４.４　環 R のイデアルが有限個の元で生成されるとき，**有限生成イデアル**という。特にイデアルがただ１つの元で生成されるとき**単項イデアル**という。

例１）$\mathbb{Z}_6$ は環であり，そのイデアルは次のものです。

$$I_1 = \mathbb{Z}_6, \quad I_2 = \{0,2,4\}, \quad I_3 = \{0,3\}, \quad I_6 = \{0\}$$

これらのイデアルの関係は，

$$I_6 \subset I_3 \subset I_1$$

$$I_6 \subset I_2 \subset I_1$$

です。特に I_6 は，下のように**可約イデアル**（Reducible Ideal）の３条件を満たすものです。

$$I_6 = I_2 \cap I_3, \quad I_6 \subsetneq I_2, \quad I_6 \subsetneq I_3$$

例２）環$\mathbb{Z}_8$のイデアルは次のようなものです。

$$I_1 = \mathbb{Z}_8, \quad I_2 = \{0,2,4,6\}, \quad I_4 = \{0,4\}, \quad I_0 = \{0\}$$

この包含関係は,

$$I_0 \subset I_4 \subset I_2 \subset I_1$$

です。

命題１４.５　$\mathbb{Z}_m$の任意のイデアルは単項イデアルである。

証明　Iを$\mathbb{Z}_m$の$\{0\}$でないイデアルとする。$I-0$の中で最小なものをαとする。$b \in I$とすると，$b = q\alpha + r,\quad 0 \le r \le \alpha - 1$と書ける。$r = b - \alpha q \in I$であり，$\alpha$の最小性から$r = 0$である。よって，$I = (\alpha)$である。□

【練習１６】環$\mathbb{Z}_{15}$のイデアルを全て書け。

定義１４.６　Rを環，イデアル$I \subset R$が**準素イデアル**であるとは，
$ab \in I, b \notin I$のとき，$a^n \in I$となる自然数nが存在することである。

例３）例２で扱ったイデアルは全て準素イデアルである。

実は，ＦＦＴにおけるビットリバースと準素イデアルが関係しているのです。そのことを 4 点ＦＦＴ，8 点ＦＦＴで説明します。

4 点ＦＦＴを考えるとき, 環は$\mathbb{Z}_4$を考えます。この準素イデアルは, $\mathbb{Z}_4$と$I_2 = \{0,2\},\quad I_0 = \{0\}$です。

先ず$\mathbb{Z}_4$をI_2で分類します。つまり，I_2に入っているものと，入っていないものに分類できます。そして入っているものを0で，入っていないものを1と表すことにします。このことを，$\mathbb{Z}_4 / I_2 = \{0,1\}$と書きます。つまり，$\mathbb{Z}_4 = \{0,2,1,3\}$と並べ替えて最初の２つが０，後の２つが１を表すのです。同様にI_2をI_0で分類すると，$I_2 / I_0 = \{0,1\}$，$I_2 + 1 = \{1,3\}$は-1することでI_2になるので，$I_2 + 1$とI_2を同じと考えて，$(I_2 + 1)/I_0 = \{0,1\}$とします。

この様子をみると, 0は最初の分類で0に次の分類で0に, 1は最初の分類で1に次の分類で0になります。図式化すると,

$$0 \to 00 \leftrightarrow 0, \quad 1 \to 10 \leftrightarrow 2, \quad 2 \to 01 \leftrightarrow 1, \quad 3 \to 11$$

という関係が見えてきます。

8 点ＦＦＴでも同様に考えてみます。この場合は，例２で扱った環とその準素イデアルで考えます。

$$\mathbb{Z}_8 / I_2 = \{I_2, I_2 + 1\} = \{0,1\}, \quad I_2 / I_4 = \{I_4, I_4 + 1\} = \{0,1\}, \quad I_4 / I_0 = \{I_0, I_0 + 1\} = \{0,1\}$$

と順次分類していくと,

$$0 \to 000 \leftrightarrow 0, \quad 1 \to 100 \leftrightarrow 4, \quad 2 \to 010 \leftrightarrow 2, \quad 3 \to 110 \leftrightarrow 6,$$
$$4 \to 001 \leftrightarrow 1, \quad 5 \to 101 \leftrightarrow 5, \quad 6 \to 011 \leftrightarrow 3, \quad 7 \to 111 \leftrightarrow 7$$

となります。ここで，$S/T = \{T, T+1\}$の$T+1$はSの中でTの集合全てに＋１した集合を意味します。

以上のことから，n点ＦＦＴにおけるビットリバースは環と準素イデアルに大きく関係していると考えられます。

【練習１７】環$\mathbb{Z}_{16}$の準素イデアルとビットリバースの様子を示せ。

一般に次の行列を定義します。

定義１４.７

①　与えられた演算$\bullet$に対して行列の演算を

$$\begin{bmatrix} x \\ y \end{bmatrix}\cdot\begin{pmatrix} a & b \\ c & d \end{pmatrix}\overset{def}{=}\begin{pmatrix} a\bullet x & b\bullet x \\ c\bullet y & d\bullet y \end{pmatrix},\qquad \alpha\begin{bmatrix} x \\ y \end{bmatrix}\overset{def}{=}\begin{bmatrix} \alpha x \\ \alpha y \end{bmatrix}$$

とする。(これは以前定義したが，今後演算$\bullet$は$+$などでもよいということを意味する.)

②　成分がm次正方行列であるn次正方行列$S=\left(S_{ij}\right)$と単なるn次正方行列$T=\left(T_{ij}\right)$について，

$$S^{\odot T}\overset{def}{=}\left([T_{ij}]\cdot S_{ij}\right)$$

とする。ここで，$\left[a\right]=\begin{bmatrix} a \\ \vdots \\ a \end{bmatrix}$を意味する。

今後のために，$I_{p^{n-1}}$，$I_{p^{n-k}}+jp^{n-1-k}$，$I_{p^{n-1-k}}$にそれぞれ対応する次の基本的な次の行列を定義します。

（１）　　　$$e\overset{def}{=}p^{n-1}\begin{bmatrix} 0 \\ 1 \\ 2 \\ \vdots \\ p-1 \end{bmatrix}\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 2 & \cdots & (p-1) \\ 0 & 1 & 2 & \cdots & (p-1) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 1 & 2 & \cdots & (p-1) \end{pmatrix}$$

（２）　　　$$B_k{}^j\overset{def}{=}\left(jp^{n-1-k}\begin{bmatrix} 0 \\ 1 \\ 2 \\ \vdots \\ (p^k-1) \end{bmatrix}+e_{k-1}\right)$$

$$(j=1,2,\cdots,p-1,\quad k=1,2,\cdots,n-1,\quad e_0=e)$$

特に$j=1$のときはB_kと書く。

（３）　　　$$e_k\overset{def}{=}\begin{pmatrix} e_{k-1} & B_k{}^1 & \cdots & B_k{}^{p-1} \\ e_{k-1} & B_k{}^1 & \cdots & B_k{}^{p-1} \\ e_{k-1} & B_k{}^1 & \cdots & B_k{}^{p-1} \\ e_{k-1} & B_k{}^1 & \cdots & B_k{}^{p-1} \end{pmatrix}^{\oplus e_{k-1}}$$

$$(j=1,2,\cdots,p-1,\quad k=1,2,\cdots,n-1,\quad e_0=e)$$

上の行列はＦＦＴを構成する行列成分のWを添え字を扱っています．したがって上の行列に対応するＦＦＴの行列があります.

具体的には，$e_k=\left(\varepsilon_{ij}\right)$ に対応する行列は$W_{e_k}=\left(W^{\varepsilon_{ij}}\right)$であり，$B_k^j=\left(\beta_{lm}\right)$に対応する行列は，$W_{B_k^j}=\left(W^{\beta_{lm}}\right)$となります．

定義１４.８　環$\mathbb{Z}_{p^n}$とその準素イデアルに対して，e_{n-1}から作った$W_{e_{n-1}}$をp^n点ＦＦＴという。

さて，$\mathbb{Z}_{2^4}$における準素イデアルは，

$$I_1=\mathbb{Z}_{16},\ \ I_2=\{0,2,4,6,8,10,12,14\},\quad I_4=\{0,4,8,12\},\quad I_8=\{0,8\},\quad I_0=\{0\}$$

です。そしてI_8に対応する行列e，　$I_{2^{4-k}}+2^{3-k}$に対応する行列B_k，$I_{2^{3-k}}$に対応するe_kは以下の通りです。

$$e=\begin{pmatrix}0 & 0\\ 0 & 8\end{pmatrix},\qquad B_1=\begin{bmatrix}0\\4\end{bmatrix}+e,\qquad e_1=\begin{pmatrix}e & B_1\\ e & -B_1\end{pmatrix},$$

$$B_2=\begin{bmatrix}0\\2\\4\\6\end{bmatrix}+e_1,\qquad e_2=\begin{pmatrix}e_1 & B_2\\ e_1 & -B_2\end{pmatrix},\qquad B_3=\begin{bmatrix}0\\1\\2\\3\\4\\5\\6\\7\end{bmatrix}+e_2,\qquad e_3=\begin{pmatrix}e_2 & B_3\\ e_2 & -B_3\end{pmatrix}$$

です。これらにより，16点ＦＦＴはW_{e_3}であり，これによりＤＦＴの$\left(c_j\right)$の計算の演算回数を減少できます。次の図を見てください

$$\begin{pmatrix}C_0\\C_1\\C_2\\C_3\\C_4\\C_5\\C_6\\C_7\\C_8\\C_9\\C_{10}\\C_{11}\\C_{12}\\C_{13}\\C_{14}\\C_{15}\end{pmatrix}=W_{e_3}\begin{pmatrix}f_0\\f_8\\f_4\\f_{12}\\f_2\\f_{10}\\f_6\\f_{14}\\f_1\\f_9\\f_5\\f_{13}\\f_3\\f_{11}\\f_7\\f_{15}\end{pmatrix}=\left(\begin{matrix}W_{e_2}\begin{pmatrix}f_0\\f_8\\f_4\\f_{12}\\f_2\\f_{10}\\f_6\\f_{14}\end{pmatrix}+W_{B_3}\begin{pmatrix}f_1\\f_9\\f_5\\f_{13}\\f_3\\f_{11}\\f_7\\f_{15}\end{pmatrix}\\ W_{e_2}\begin{pmatrix}f_0\\f_8\\f_4\\f_{12}\\f_2\\f_{10}\\f_6\\f_{14}\end{pmatrix}-W_{B_3}\begin{pmatrix}f_1\\f_9\\f_5\\f_{13}\\f_3\\f_{11}\\f_7\\f_{15}\end{pmatrix}\end{matrix}\right)=\left(\begin{matrix}\begin{pmatrix}W_{e_1}\begin{pmatrix}f_0\\f_8\\f_4\\f_{12}\end{pmatrix}+W_{B_2}\begin{pmatrix}f_2\\f_{10}\\f_6\\f_{14}\end{pmatrix}\\ W_{e_1}\begin{pmatrix}f_0\\f_8\\f_4\\f_{12}\end{pmatrix}-W_{B_2}\begin{pmatrix}f_2\\f_{10}\\f_6\\f_{14}\end{pmatrix}\end{pmatrix}+W_{B_3}\begin{pmatrix}f_1\\f_9\\f_5\\f_{13}\\f_3\\f_{11}\\f_7\\f_{15}\end{pmatrix}\\ \begin{pmatrix}W_{e_1}\begin{pmatrix}f_0\\f_8\\f_4\\f_{12}\end{pmatrix}+W_{B_2}\begin{pmatrix}f_2\\f_{10}\\f_6\\f_{14}\end{pmatrix}\\ W_{e_1}\begin{pmatrix}f_0\\f_8\\f_4\\f_{12}\end{pmatrix}-W_{B_2}\begin{pmatrix}f_2\\f_{10}\\f_6\\f_{14}\end{pmatrix}\end{pmatrix}-W_{B_3}\begin{pmatrix}f_1\\f_9\\f_5\\f_{13}\\f_3\\f_{11}\\f_7\\f_{15}\end{pmatrix}\end{matrix}\right)$$

$$
=\begin{pmatrix}
\begin{matrix}
\begin{matrix}
W_e\begin{pmatrix}f_0\\f_8\end{pmatrix}+W_{B_1}\begin{pmatrix}f_4\\f_{12}\end{pmatrix}\\
W_e\begin{pmatrix}f_0\\f_8\end{pmatrix}-W_{B_1}\begin{pmatrix}f_4\\f_{12}\end{pmatrix}
\end{matrix}
+W_{B_2}\begin{pmatrix}f_2\\f_{10}\\f_6\\f_{14}\end{pmatrix}\\
\begin{matrix}
W_e\begin{pmatrix}f_0\\f_8\end{pmatrix}+W_{B_1}\begin{pmatrix}f_4\\f_{12}\end{pmatrix}\\
W_e\begin{pmatrix}f_0\\f_8\end{pmatrix}-W_{B_1}\begin{pmatrix}f_4\\f_{12}\end{pmatrix}
\end{matrix}
-W_{B_2}\begin{pmatrix}f_2\\f_{10}\\f_6\\f_{14}\end{pmatrix}
\end{matrix}
+W_{B_3}\begin{pmatrix}f_1\\f_9\\f_5\\f_{13}\\f_3\\f_{11}\\f_7\\f_{15}\end{pmatrix}\\
\begin{matrix}
\begin{matrix}
W_e\begin{pmatrix}f_0\\f_8\end{pmatrix}+W_{B_1}\begin{pmatrix}f_4\\f_{12}\end{pmatrix}\\
W_e\begin{pmatrix}f_0\\f_8\end{pmatrix}-W_{B_1}\begin{pmatrix}f_4\\f_{12}\end{pmatrix}
\end{matrix}
+W_{B_2}\begin{pmatrix}f_2\\f_{10}\\f_6\\f_{14}\end{pmatrix}\\
\begin{matrix}
W_e\begin{pmatrix}f_0\\f_8\end{pmatrix}+W_{B_1}\begin{pmatrix}f_4\\f_{12}\end{pmatrix}\\
W_e\begin{pmatrix}f_0\\f_8\end{pmatrix}-W_{B_1}\begin{pmatrix}f_4\\f_{12}\end{pmatrix}
\end{matrix}
-W_{B_2}\begin{pmatrix}f_2\\f_{10}\\f_6\\f_{14}\end{pmatrix}
\end{matrix}
-W_{B_3}\begin{pmatrix}f_1\\f_9\\f_5\\f_{13}\\f_3\\f_{11}\\f_7\\f_{15}\end{pmatrix}
\end{pmatrix}
$$

【課題１１】　36 点 FFT を求めよ。

次は3^n点ＦＦＴを考えてみましょう。例えば，９点ＦＦＴを考えます。この場合，$\mathbb{Z}_9$でその準素イデアルは，$I_3=\{0,3,6\}$，$I_0=\{0\}$です。このことから，先ほどと同じように，分類すると，

$$\mathbb{Z}_9/I_3=\{I_3, I_3+1, I_3+2\}=\{0,1,2\},\quad I_3/I_0=\{I_0, I_0+1, I_0+2\}=\{0,1,2\}$$

となり，

$$0\to 00\leftrightarrow 0,\quad 1\to 10\leftrightarrow 3,\quad 2\to 20\leftrightarrow 6,\quad 3\to 01\leftrightarrow 1,$$

$$4\to 11\leftrightarrow 4,\quad 5\to 21\leftrightarrow 7,\quad 6\to 02\leftrightarrow 2,\quad 7\to 12\leftrightarrow 5,\quad 8\to 22\leftrightarrow 8$$

となります。

以前使った添え字だけの行列を書いてみると，まず,

$$A=\begin{pmatrix}
0&0&0&0&0&0&0&0&0\\
0&1&2&3&4&5&6&7&8\\
0&2&4&6&8&1&3&5&7\\
0&3&6&0&3&6&0&3&6\\
0&4&8&3&7&2&6&1&5\\
0&5&1&6&2&7&3&8&4\\
0&6&3&0&6&3&0&6&3\\
0&7&5&3&1&8&6&4&2\\
0&8&7&6&5&4&3&2&1
\end{pmatrix}$$

を得ます。これも対称行列です。次に上で分類したように並べ替えます。

$$A' = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 & 8 \\ 0 & 6 & 3 & 2 & 8 & 5 & 4 & 1 & 7 \\ 0 & 0 & 0 & 3 & 3 & 3 & 6 & 6 & 6 \\ 0 & 3 & 6 & 4 & 7 & 1 & 8 & 2 & 5 \\ 0 & 6 & 3 & 5 & 2 & 8 & 1 & 7 & 4 \\ 0 & 0 & 0 & 6 & 6 & 6 & 3 & 3 & 3 \\ 0 & 3 & 6 & 7 & 1 & 4 & 5 & 8 & 2 \\ 0 & 6 & 3 & 8 & 5 & 2 & 7 & 4 & 1 \end{pmatrix}$$

そうすると，I_3 に対応する行列と $I_3 + j$ 行列が見えてきます。
それは,

$$e = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & 6 \\ 0 & 6 & 3 \end{pmatrix}, \qquad B_1^{\,j} = \left(j \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & 6 \\ 0 & 6 & 3 \end{pmatrix} \right) \quad (j = 1, 2)$$

です。そして A' の構造は

$$A' = \begin{pmatrix} e & B_1^{\,1} & B_1^{\,2} \\ e & B_1^{\,1} & B_1^{\,2} \\ e & B_1^{\,1} & B_1^{\,2} \end{pmatrix}^{\oplus e} = \begin{pmatrix} e & B_1^{\,1} & B_1^{\,2} \\ e & [3] + B_1^{\,1} & [6] + B_1^{\,2} \\ e & [6] + B_1^{\,1} & [3] + B_1^{\,2} \end{pmatrix}$$

となっています。そこで，行列 $e, B_1^{\,j}$ らを $W_e, W_{B_1^{\,j}}$ に置き換えて計算することがＦＦＴであり，これによって演算回数は減少します。

さて，環 R における準素イデアルの中で $\{0\}$ の次に小さなものを**最小準素イデアル**ということにします，$\mathbb{Z}_4$ の最小準素イデアルは，$I_2 = \{0, 2\}$ で，$\mathbb{Z}_8$ においては，$I_4 = \{0, 4\}$，$\mathbb{Z}_9$ においては，$I_3 = \{0, 3, 6\}$ でした。そして I_k $(k = 2, 4, 3)$ に対応する行列は，それぞれ,

$$\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 4 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & 6 \\ 0 & 6 & 3 \end{pmatrix}$$

でした。3^3 点ＦＦＴも同様です。この場合は，$\mathbb{Z}_{27}$ で，準素イデアルは,

$$\mathbb{Z}_{27,} \qquad I_3 = \{0, 3, 6, 9, 12, 15, 18, 21, 24\}, \quad I_9 = \{0, 9, 18\}, \quad I_0 = \{0\}$$

であり，I_9 に対応する行列 e は,

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 9 & 18 \\ 0 & 18 & 9 \end{pmatrix}$$

でした。

次の定理は最初のＤＦＴの行列が対称行列であることと，それを準素イデアルで置換することと，数学的帰納法により証明されます。

定理１４.９　p を素数，$n \geqq 2$ の整数としたとき，$I_{p^{n-1}}$ に対応する行列 e，$I_{p^{n-k}}$ に対応する行列 e_k，$I_{p^{n-k}} + jp^{n-1-k}$ に対応する行列 $B_k{}^j$ により，離散フーリエ係数が与えられる。

【課題１２】　27 点ＦＦＴを示せ。

＊上に説明したＦＦＴは基本的なものですが，巡回形の構造を使うことによりもう少し高速に行うこともできます。また 15 点や 36 点なども準素イデアルを考えることでやはりＦＦＴを考えることができます。「やさしいフーリエ変換，松尾博著，森北出版」等を参考にして下さい。

＊　第４回レポート提出について。 【課題１０】～【課題１２】の中から好きな課題を１つ選んでレポートとして提出せよ。