Lecture 18.

At some point we touched base on the following question. Let $m,n \in \mathbb{Z}_{>1}$ be coprime, i.e. $\gcd(m,n)=1$. Then the two abelian groups, $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ are isomorphic via $\varphi: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ with $\varphi(1)=(1,1)$ (so $\varphi(k)=(k \pmod m, k \pmod n)$). There are 2 ways we can define discrete Fourier transform: directly, using the matrix

$$F_{mn} = \frac{1}{\sqrt{mn}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{mn-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{mn-1} & \cdots & \omega^{(mn-1)^2} \end{pmatrix} \quad \text{with } \omega = e^{2\pi i/mn}$$

or as $F_m \otimes F_n$ with

$$F_m = \frac{1}{\sqrt{m}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_1 & \cdots & \omega_1^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_1^{m-1} & \cdots & \omega_1^{(m-1)^2} \end{pmatrix}, \quad F_n = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_2 & \cdots & \omega_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_2^{n-1} & \cdots & \omega_2^{(n-1)^2} \end{pmatrix} \quad \begin{array}{l} \omega_1 = e^{2\pi i/m} \\ \omega_2 = e^{2\pi i/n}. \end{array}$$

We shall compare the two: let $t \in \mathbb{Z}_{mn}$, then

$$F_{nm}(\delta_t) = \frac{1}{\sqrt{nm}} \sum_{b=0}^{nm-1} \omega^{tb} |\delta_b\rangle = \frac{1}{\sqrt{nm}} \sum_{b=0}^{nm-1} \omega^{tb} |\delta_{b \pmod m}\rangle \otimes |\delta_{b \pmod n}\rangle$$

Recall that $\gcd(m,n)=1$ implies that $\exists c,d \in \mathbb{Z}$ with

$$\boxed{cm + dn = 1.}$$

Hence $\omega^{tb} = \omega^{(cm+dn)tb} = \omega^{cmtb} \cdot \omega^{dntb} = \omega_2^{ctb} \cdot \omega_1^{dtb} = \omega_1^{dtb}\, \omega_2^{ctb}.$

Therefore, $\frac{1}{\sqrt{nm}} \sum_{b=0}^{nm-1} \omega^{tb} |\delta_{b \pmod m}\rangle \otimes |\delta_{b \pmod n}\rangle =$

$$= \frac{1}{\sqrt{nm}} \sum_{b=0}^{nm-1} \omega_1^{dtb} |\delta_{b \pmod m}\rangle \otimes \omega_2^{ctb} |\delta_{b \pmod n}\rangle =$$

$$= \frac{1}{\sqrt{m}} \sum_{s=0}^{m-1} \omega_1^{dts} |\delta_s\rangle \otimes \frac{1}{\sqrt{n}} \sum_{l=0}^{n-1} \omega_2^{ctl} |\delta_l\rangle =$$

$$= F_m(\delta_{dt \pmod m}) \otimes F_n(\delta_{ct \pmod n}).$$

<u>Rmk.</u> As c and d satisfy the equation $cm+dn=1$, we have that d is invertible modulo m (the inverse is $n \pmod m$) and c is invertible modulo n (the inverse is $m \pmod n$).

<u>Conclusion</u>: the matrices of F_{mn} and $F_m \otimes F_n$ differ by a permutation of columns determined by c and d.

<u>Example.</u> Let's compare F_6 with $F_3 \otimes F_2$. As $\gcd(2,3)=1=1\cdot 3+(-1)\cdot 2$, we get $c=1$, $d=-1$. Therefore, the permutation induced by c on $\mathbb{Z}_2$ is trivial, while the permutation induced by d on $\mathbb{Z}_3$ maps 0 to $-1\cdot 0=0$, and exchanges 1 and 2:

$$-1\cdot 1=-1\equiv 2 \pmod 3) \text{ and } -1\cdot 2\equiv -2\equiv 1 \pmod 3).$$

As $\varphi(0)=(0,0)$
$\varphi(1)=(1,1)$
$\varphi(2)=(0,2)$
$\varphi(3)=(1,0)$
$\varphi(4)=(0,1)$, $\varphi(5)=(1,2)$, we get that the columns $1,5$ should be swapped and same for columns $2,4$, in

order to match F_6 and $F_2 \otimes F_3$. Let's check it.

$$F_6 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 \\ 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 \\ 1 & \omega^3 & 1 & \omega^3 & 1 & \omega^3 \\ 1 & \omega^4 & \omega^2 & 1 & \omega^4 & \omega^2 \\ 1 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix} \qquad \omega = e^{2\pi i/6}$$

$$F_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{pmatrix} \qquad \zeta = e^{2\pi i/3}$$

$$F_2 \otimes F_3 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -\zeta & \zeta^2 & -1 & \zeta & -\zeta^2 \\ 1 & \zeta^2 & \zeta & 1 & \zeta^2 & \zeta \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & \zeta & \zeta^2 & 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta & -1 & \zeta & -\zeta \end{pmatrix}$$

As $\omega^3 = e^{6\pi i/6} = e^{\pi i} = -1$ and $\omega = -\zeta^2$, the assertion follows.