Proof of Lem. 7.8. For any $m \in \mathbb{P}$, we let ρ_m denote the rotation on Q^m (i.e., the map $Q^m \to Q^m$, $(q_1, q_2, \ldots, q_m) \mapsto (q_2, q_3, \ldots, q_m, q_1)$). This was formerly called ρ.

We have $n = km$ for some $m \in \mathbb{P}$ (since $k \mid n$). Consider this m.

The map

$$M: \quad Q^k \longrightarrow Q^n,$$
$$(q_1, q_2, \ldots, q_k) \longmapsto (\underbrace{q_1, q_2, \ldots, q_k, q_1, q_2, \ldots, q_k, \ldots\ldots, q_1, q_2, \ldots, q_k}_{m \text{ times } q_1, q_2, \ldots, q_k}).$$

It is easy to see: $M \circ \rho_k = \rho_n \circ M$.

Thus, M sends each cycle of ρ_k to a cycle of ρ_n (i.e., if C is a cycle of ρ_k, then $M(C)$ is a cycle of ρ_n).

Moreover, M preserves the sizes (= periods) of these cycles (since M is injective). Thus, we get a map

$$\overline{M}: Q^k_{\text{neck},k} \to Q^n_{\text{neck},k}, \qquad C \mapsto M(C).$$

This $\overline{M}$ is injective (since M is injective).

Claim. 1: Also, $\overline{M}$ is surjective.

[Proof: Let $C \in Q^n_{neck,k}$. Pick any $\vec{q} \in C$.

Then, the cycle of ρ_n containing $\vec{q}$ is C, and thus has size $|C| = k$ (since $C \in Q^n_{neck,k}$).

Hence, $\rho^k_n(\vec{q}) = \vec{q}$.

Thus, $\vec{q} = (q_1, q_2, \ldots, q_k, q_1, q_2, \ldots, q_k, \ldots, q_1, q_2, \ldots, q_k)$

for some $q_1, q_2, \ldots, q_k \in Q$.

Hence, $\vec{q} = M(\vec{r})$ for some $\vec{r} \in Q^k$.

Also, the cycle of ρ_k containing $\vec{r}$ goes to the cycle of ρ_n containing $\vec{q}$ under M, and thus has the same size as the latter (since M is injective). But the latter has size k. Thus, the former has size k, too.

So it belongs to $Q^k_{neck,k}$. Its image under $\overline{M}$ is C.

Thus, C is an image under $\overline{M}$.

Since we have proven this $\forall\, C \in Q^n_{neck,k}$,

we thus conclude that $\overline{M}$ is surjective.]

Now, $\overline{M}$ is injective & surjective, thus bijective.

$\Longrightarrow \quad |Q^k_{neck,k}| = |Q^n_{neck,k}|$. $\square$

Lem. 7.10. Let Q be a finite set. Let $q = |Q|$. Then, $\forall\, n \in \mathbb{P}$,

$$q^n = \sum_{d \mid n} d\, |Q^d_{neck,d}|$$

Proof. $q^n = |Q^n| = \sum_{C \text{ is a cycle of } \rho} |C|$ (since Q^n is the disjoint union of the cycles of ρ)

$$= \sum_{C \in Q^n_{neck}} |C| = \sum_{d \mid n} \sum_{C \in Q^n_{neck,d}} \underbrace{|C|}_{\substack{= d \\ (\text{since } C \in Q^n_{neck,d})}}$$ (by Cor. 7.7)

$$= \sum_{d \mid n} \underbrace{\sum_{C \in Q^n_{neck,d}} d}_{= d\,|Q^n_{neck,d}|} = \sum_{d \mid n} d\, \underbrace{|Q^n_{neck,d}|}_{\substack{= |Q^d_{neck,d}| \\ \text{(by Lem. 7.8)}}}$$

$$= \sum_{d \mid n} d\,|Q^d_{neck,d}|.$$

$\square$

Proof of Thm. 7.9. (2) ~~Theorem~~ Lem. 7.10 yields

$$q^n = \sum_{d \mid n} d\,|Q^d_{neck,d}| \qquad \forall n \in \mathbb{P}.$$

Thus, Thm. 7.4 (applied to $a_n = q^n$ and $b_n = n\,|Q^n_{neck,n}|$) yields

$$n\,|Q^n_{neck,n}| = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d \qquad \forall n \in \mathbb{P}.$$

Dividing this by n, we get

$$|Q^n_{neck,n}| = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d \mid n} \mu(d)\, q^{n/d}$$

(here, we substituted d for n/d in the sum, since the map $\begin{array}{c}\{\text{positive divisors of } n\} \to \{\text{positive divisors of } n\}, \\ d \mapsto n/d\end{array}$ is a bijection).

(b) Cor. 7.7 yields that Q^n_{neck} is the union of its subsets $Q^n_{neck,d}$ for $d \mid n$. Since these subsets are disjoint, this yields

$$|Q^n| = \sum_{d\mid n} |Q^n_{neck,d}| = \sum_{k\mid n} \underbrace{|Q^n_{neck,k}|}_{\substack{=|Q^k_{neck,k}| \\ \text{(by Lem. 7.8)}}}$$

$$= \sum_{k\mid n} \underbrace{|Q^k_{neck,k}|}_{=\frac{1}{k}\sum_{d\mid k}\mu\left(\frac{k}{d}\right)q^d} = \underbrace{\sum_{k\mid n} \sum_{d\mid k}}_{=\sum_{d\mid n}\sum_{\substack{k\mid n; \\ d\mid k}}} \frac{1}{k}\mu\left(\frac{k}{d}\right)q^d$$

$$= \sum_{d \mid n} \underbrace{\sum_{\substack{k \mid n; \\ d \mid k}} \frac{1}{k} \mu\left(\frac{k}{d}\right)}_{= \sum_{f \mid \frac{n}{d}} \frac{1}{df} \mu\left(\frac{df}{d}\right)} q^d$$

(here, we substituted df for k, since the map

$$\{\text{pos. divisors of } \tfrac{n}{d}\} \to \{\text{pos. divisors } k \text{ of } n \mid d \mid k\},$$
$$f \mapsto df$$

is a bijection)

$$= \sum_{d \mid n} \sum_{f \mid \frac{n}{d}} \underbrace{\frac{1}{df}}_{= \frac{1}{n} \cdot \frac{n/d}{f}} \mu\Big(\underbrace{\frac{df}{d}}_{=f}\Big) q^d = \sum_{d \mid n} \frac{1}{n} \underbrace{\sum_{f \mid \frac{n}{d}} \frac{n/d}{f} \mu(f)}_{= \phi(n/d)} q^d$$

(by Prop. 7.5, applied to n/d instead of n)

$$= \sum_{d|n} \frac{1}{n} \phi(n/d)\, q^d = \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) q^d$$

$$= \frac{1}{n} \sum_{d|n} \phi(d)\, q^{n/d}$$ (here, we substituted n/d for d).

$\square$

(c) LTTR (similar to (b)).

<u>Cor. 7.11.</u> ~~(a)~~ Let $q \in \mathbb{Z}$ and $n \in \mathbb{P}$.

(a) We have $n \mid \sum_{d|n} \mu(d)\, q^{n/d}$;

(b) We have $n \mid \sum_{d|n} \phi(d)\, q^{n/d}$.

(c) We have ~~q~~ $q^n \equiv q \mod n$ if n is prime. (Fermat's Little Theorem).

<u>Proof.</u> WLOG assume $q \geq 0$, since we can otherwise replace q by the remainder of q modulo n (which is $\equiv q \mod n$, but is ≥ 0). Hence $\exists$ finite set Q such that $|Q| = q$. Consider this q.

Thus, Thm. 7.9 (a) yields

$$|Q^n_{\text{neck},n}| = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d .$$

Hence, $\sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d = n \cdot \underbrace{|Q^n_{\text{neck},n}|}_{\in \mathbb{Z}}$, and this clearly is divisible by n. This proves Cor. 7.11 (a).

Same argument proves Cor. 7.11 (b), but now use Thm. 7.9 (b).

(c) Assume: n is prime.

Then, (a) yields $n \mid \sum_{d \mid n} \mu(d) q^{n/d} \overset{\text{since } n \text{ is prime}}{=} \underbrace{\mu(1)}_{=1} \underbrace{q^{n/1}}_{=q^n} + \underbrace{\mu(n)}_{=-1} \underbrace{q^{n/n}}_{=q^1 = q}$

$= q^n - q$, so that $q^n \equiv q \mod n$. $\square$

8. Generating functions

8.1. Examples

Let me show what generating functions ("gfs") are good for. Then, in §8.2 onwards, I'll explain how to define them. For now, we work informally; please suspend your disbelief.

Basic idea: Any sequence $(a_0, a_1, a_2, \ldots)$ of numbers gives rise to a "power series" $a_0 + a_1 x + a_2 x^2 + \cdots$, called its "generating function". What does this mean? See later (& see also [Loehr, Ch. 7 (1st edition)], or [Niven, "Formal Power Series"]).

Example 1: Recall the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$ with $f_0 = 0$ & $f_1 = 1$ & $f_n = f_{n-1} + f_{n-2}$.

Consider its gf
$$F(x) = f_0 + f_1 x + f_2 x^2 + \cdots$$
$$= 0 + 1x + 1x^2 + 2x^3 + 3x^4 + \cdots,$$

Then,

$$F(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + \cdots$$

$$= 0 + 1\,x + (f_0+f_1)x^2 + (f_1+f_2)x^3 + (f_2+f_3)x^4 + \cdots$$

$$= x + \underbrace{\left(f_0 x^2 + f_1 x^3 + f_2 x^4 + \cdots\right)}_{= x^2F(x)}$$

$$+ \underbrace{\left(f_1 x^2 + f_2 x^3 + f_3 x^4 + \cdots\right)}_{= f_0 x + f_1 x^2 + f_2 x^3 + f_3 x^4 + \cdots \; = xF(x)}$$

(since $f_0 = 0$)

$$= x + x^2F(x) + xF(x) = x + (x+x^2)F(x).$$

Solving this for $F(x)$, we get

$$F(x) = \frac{x}{1-x-x^2} = \frac{x}{(1-\phi_1 x)(1-\phi_2 x)},$$

where $\phi_1 = (1+\sqrt{5})/2$

and $\phi_2 = (1-\sqrt{5})/2$

are the "golden ratios".

Applying partial fraction decomposition to the RHS, we obtain

$$F(x) = \frac{1}{\sqrt{5}} \cdot \frac{1}{1-\phi_1 x} - \frac{1}{\sqrt{5}} \cdot \frac{1}{1-\phi_2 x}, \tag{71}$$

Now, what are the coefficients of $\frac{1}{1-\alpha x}$ for $\alpha \in \mathbb{C}$?

Well: $$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots$$

(since $(1-x)(1+x+x^2+x^3+\cdots)$
$= (1+\cancel{x}+\cancel{x^2}+\cancel{x^3}+\cancel{\cdots}) - (\cancel{x}+\cancel{x^2}+\cancel{x^3}+\cancel{x^4}+\cdots) = 1$).

So, if we substitute αx for x here, we get

$$\frac{1}{1-\alpha x} = 1 + \alpha x + (\alpha x)^2 + (\alpha x)^3 + \cdots$$
$$= 1 + \alpha x + \alpha^2 x^2 + \alpha^3 x^3 + \cdots .$$

Thus, (71) becomes

$$F(x) = \frac{1}{\sqrt{5}} (1 + \phi_1 x + \phi_1^2 x^2 + \phi_1^3 x^3 + \cdots)$$

$$-\frac{1}{\sqrt{5}}\left(1+\phi_2 x+\phi_2^2 x^2+\phi_2^3 x^3+\cdots\right)$$

$$=\left(\frac{1}{\sqrt{5}}\cdot 1-\frac{1}{\sqrt{5}}\cdot 1\right)+\left(\frac{1}{\sqrt{5}}\phi_1-\frac{1}{\sqrt{5}}\phi_2\right)x$$

$$+\left(\frac{1}{\sqrt{5}}\phi_1^2-\frac{1}{\sqrt{5}}\phi_2^2\right)x^2+\cdots.$$

Now, comparing coefficients before x^n, we get

$$\boxed{f_n=\frac{1}{\sqrt{5}}\phi_1^n-\frac{1}{\sqrt{5}}\phi_2^n}$$

(Binet's formula).

(This has many consequences, e.g., that

$$\lim_{n\to\infty}\frac{f_{n+1}}{f_n}=\phi_1=\frac{1+\sqrt{5}}{2}\approx 1.618\ldots\ .)$$

<u>Example 2:</u> For each $n\in\mathbb{N}$, define the Catalan number C_n as the # of legal LPs from $(0,0)$ to (n,n) (using the notation of ~~§~~ §6.2). Let's pretend we do NOT know that $C_n=\frac{1}{n+1}\binom{2n}{n}=\binom{2n}{n}-\binom{2n}{n-1}$. How do we

come up with such a formula?

Let $C(x) = C_0 + C_1 x + C_2 x^2 + C_3 x^3 + \dots = \sum_{n \geq 0} C_n x^n$.

Cor. 6,4 yields $C_n = \sum_{k=1}^{n} C_{k-1} C_{n-k}$.

Thus, $C(x) = 1 + C_0 C_0 x + (C_0 C_1 + C_1 C_0) x^2$
$+ (C_0 C_2 + C_1 C_1 + C_2 C_0) x^3$
$+ (C_0 C_3 + C_1 C_2 + C_2 C_1 + C_3 C_0) x^4 + \dots$

$$= 1 + x \big(\underbrace{C_0 + C_1 x + C_2 x^2 + \dots}_{= C(x)} \big)^2$$

(since $(a_0 + a_1 x + a_2 x^2 + \dots)^2$
$= (a_0 + a_1 x + a_2 x^2 + \dots) \cdot (a_0 + a_1 x + a_2 x^2 + \dots)$
$= a_0 a_0 + a_0 a_1 x + a_0 a_2 x^2 + \dots$
$+ a_1 x a_0 + a_1 x a_1 x + a_1 x a_2 x^2 + \dots$
$+ a_2 x^2 a_0 + a_2 x^2 a_1 x + a_2 x^2 a_2 x^2 + \dots$
$+ \dots$

$$= a_0 a_0 + (a_0 a_1 + a_1 a_0)x + (a_0 a_2 + a_1 a_1 + a_2 a_0)x^2 + (a_0 a_3 + a_1 a_2 + a_2 a_1 + a_3 a_0)x^3 + \cdots$$

for any numbers $a_0, a_1, a_2, \ldots$).

So we have $C(x) = 1 + x \cdot (C(x))^2$.

This is a quadratic equation in $C(x)$. Solving it, we get

$$C(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

The $\pm$ cannot be a $+$, since with a $+$ the power series on top of the fraction would not be divisible by $2x$. So,

(72) $$C(x) = \frac{1-\sqrt{1-4x}}{2x} = \frac{1}{2x}\left(1-(1-4x)^{1/2}\right).$$

But recall $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k = \sum_{k \geq 0} \binom{n}{k} x^k$.

Let's pretend this works for $n = 1/2$, too. Thus,

$$(1+x)^{1/2} = \sum_{k\geq 0} \binom{1/2}{k} x^k .$$

Now, ~~//~~ substitute $-4x$ for x here, to get

$$(1-4x)^{1/2} = \sum_{k\geq 0} \binom{1/2}{k} (-4x)^k = \sum_{k\geq 0} \binom{1/2}{k} (-4)^k x^k .$$

So (72) becomes

$$C(x) = \frac{1}{2x}\Big(\underbrace{1 - \sum_{k\geq 0} \binom{1/2}{k} (-4)^k x^k}_{= - \sum_{k\geq 1} \binom{1/2}{k} (-4)^k x^k}\Big)$$

$$= - \sum_{k\geq 1} \binom{1/2}{k} \frac{(-4)^k}{2} x^{k-1}$$

$$= - \sum_{k\geq 0} \binom{1/2}{k+1} \frac{(-4)^{k+1}}{2} x^k .$$

Comparing coefficients before x^n, we obtain

$$c_n = \underbrace{-\binom{1/2}{n+1}\frac{(-4)^{n+1}}{2}}_{=2\cdot(-4)^n} = 2\cdot \underbrace{\binom{1/2}{n+1}}_{=\frac{1/2}{n+1}\binom{-1/2}{n}} \cdot (-4)^n$$

(by absorption identity)

$$= \cancel{2}\cdot\frac{\cancel{1/2}}{n+1}\underbrace{\binom{-1/2}{n}}_{=\binom{2n}{n}\cdot\left(-\frac{1}{4}\right)^n}\cdot(-4)^n = \frac{1}{n+1}\binom{2n}{n}\cancel{\left(-\frac{1}{4}\right)^n}\cancel{(-4)^n}$$

(by HW#3 exe 3(a))

$$= \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1}.$$

Thus, we have recovered Prop. 6.3 (d).

Example 3: What we have done in §2.6.

In fact, polynomials are particular case of gfs.

Example 4 (from [Wilf's "generatingfunctionology"]):

Define a sequence $(a_0, a_1, a_2, \dots)$ recursively by

$$a_0 = 1, \qquad a_{n+1} = 2a_n + n \qquad \forall n \geq 0.$$

(So it starts with $1, 2, 5, 12, 27, 58, 121, \dots$.
it is A000325 in OEIS, up to index shift.)

Set $A(x) = a_0 + a_1 x + a_2 x^2 + \dots$

Then,

$$A(x) = 1 + (2a_0 + 0)x + (2a_1 + 1)x^2 + (2a_2 + 2)x^3 + \dots$$

$$= 1 + 2(a_0 x + a_1 x^2 + a_2 x^3 + \dots)$$

$$+ (0x + 1x^2 + 2x^3 + \dots)$$

$$(74) \qquad = 1 + 2xA(x) + x\underbrace{(0 + 1x + 2x^2 + 3x^3 + \dots)}_{=?}$$

Now, what is $0 + 1x + 2x^2 + 3x^3 + \dots$?

Three ways to compute it:

①
$$0 + 1x + 2x^2 + 3x^3 + \dots$$
$$= x\underbrace{(1 + 2x + 3x^2 + \dots)}_{\begin{aligned}&= \frac{d}{dx}(1+x+x^2+\dots)\\ &= \frac{d}{dx}\left(\frac{1}{1-x}\right) = \frac{1}{(1-x)^2}\end{aligned}} = x \cdot \frac{1}{(1-x)^2} = \frac{x}{(1-x)^2}.$$

②
$$0 + 1x + 2x^2 + 3x^3 + \dots$$
$$\begin{aligned} = \quad & x + x^2 + x^3 + x^4 + \dots \\ & \phantom{x + {}} x^2 + x^3 + x^4 + \dots \\ + \quad & \phantom{x + x^2 + {}} x^3 + x^4 + \dots \\ + \quad & \phantom{x + x^2 + x^3 + {}} x^4 + \dots \\ + \quad & \dots \\ + \quad & \end{aligned}$$
$$= x \cdot \frac{1}{1-x} + x^2 \cdot \frac{1}{1-x} + x^3 \cdot \frac{1}{1-x} + \dots$$

(since $x^i + x^{i+1} + x^{i+2} + \dots = x^i \cdot \frac{1}{1-x} \quad \forall i \in \mathbb{N}$)

$$= \underbrace{\left(x + x^2 + x^3 + \cdots\right)}_{\substack{= x \cdot (1 + x + x^2 + \cdots) \\ = x \cdot \frac{1}{1-x}}} \cdot \frac{1}{1-x} = x \cdot \frac{1}{1-x} \cdot \frac{1}{1-x}$$

$$= \frac{x}{(1-x)^2}.$$

③ For any $n \in \mathbb{N}$, we have
$$0 + 1x + 2x^2 + \cdots + nx^n = \frac{x}{(1-x)^2}\left(1 - x^{n+1} - (n+1)(1-x)x^n\right)$$
(proof: induction on n). Now, take the "limit" as $n \to \infty$.

Thus, (74) becomes $A(x) = 1 + 2xA(x) + x \cdot \frac{x}{(1-x)^2}$.

This is a linear eqn. in $A(x)$. Solving it, we get

$$A(x) = \frac{1 - 2x + 2x^2}{(1-x)^2(1-2x)}$$

$$= \underbrace{\frac{-1}{(1-x)^2}}_{\substack{= -(1+2x+3x^2+\cdots) \\ \text{(by above)}}} + \underbrace{\frac{2}{1-2x}}_{\substack{= 2\sum_{k\geq 0}(2x)^k \\ = \sum_{k\geq 0} 2^{k+1}x^k}}$$

$$= -(1+2x+3x^2+\cdots) + \sum_{k\geq 0} 2^{k+1}x^k$$

$$= \sum_{k\geq 0} \left(2^{k+1} - (k+1)\right)x^k.$$

Comparing coefficients, we get $a_n = 2^{n+1} - (n+1)$.