4.11. Determinants

Def. Let $n \in \mathbb{N}$. Let A be an $n \times n$-matrix (e.g., with rational or real or complex entries). Write A as

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} = \left(a_{i,j}\right)_{i,j \in [n]}. \tag{38}$$

Then, the **determinant** $\det A$ of A is defined by

LaTeX:
```
\cdots ⋯
\rdots ⋰
\ddots ⋱
```

$$\det A = \sum_{\sigma \in S_n} (-1)^{\sigma} \underbrace{a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}}_{= \prod_{i \in [n]} a_{i,\sigma(i)} =: \operatorname{prod}_{\sigma} A}.$$

Examples: • $\det\left(a_{1,1}\right) = \sum_{\sigma \in S_1} (-1)^{\sigma} a_{1,\sigma(1)} = (-1)^{\mathrm{id}} a_{1,\mathrm{id}(1)} = a_{1,1}$.

- $$\det\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} = \underbrace{(-1)^{id}}_{=1} \underbrace{a_{1,id(1)}}_{=a_{1,1}} \underbrace{a_{2,id(2)}}_{=a_{2,2}}$$

$$+ \underbrace{(-1)^{[2,1]}}_{=-1} \underbrace{a_{1,[2,1](1)}}_{=a_{1,2}} \underbrace{a_{2,[2,1](2)}}_{=a_{2,1}}$$

(note: $[2,1]$ in one-line notation $= s_1 = w_0$)

$$= a_{1,1}a_{2,2} - a_{1,2}a_{2,1}.$$

- $$\det\begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} = ab'c'' + bc'a'' + ca'b'' - ac'b'' - ba'c'' - cb'a''$$

("Sarrus's rule").

- $\det$ (a 4×4-matrix) = (a sum of 12 products) $-$ (another sum of 12 products).

- $\det$ (the 0×0-matrix) $= 1$.

Example: I claim that if an $n \times n$-matrix A has two equal rows, then $\det A = 0$.

Proof: Let A have two equal rows.

Let row i of A be equal to row j of A, with $1 \leq i < j \leq n$.

Write A as in (38). Then,

$$a_{i,k} = a_{j,k} \qquad \forall k \in [n]. \tag{39}$$

Now, $\det A = \sum_{\sigma \in S_n} (-1)^\sigma \operatorname{prod}_\sigma A$ (by definition)

$$= \sum_{\substack{\sigma \in S_n; \\ \sigma(i) < \sigma(j)}} (-1)^\sigma \operatorname{prod}_\sigma A + \sum_{\substack{\sigma \in S_n; \\ \sigma(i) > \sigma(j)}} (-1)^\sigma \operatorname{prod}_\sigma A$$

$$= \sum_{\substack{\tau \in S_n; \\ \tau(i) > \tau(j)}} (-1)^{\tau \circ t_{i,j}} \operatorname{prod}_{\tau \circ t_{i,j}} A + \sum_{\substack{\sigma \in S_n; \\ \sigma(i) > \sigma(j)}} (-1)^\sigma \operatorname{prod}_\sigma A$$

(here, we substituted $\tau \circ t_{i,j}$ for σ in the first sum)

$$= \sum_{\substack{\sigma \in S_n; \\ \sigma(i) > \sigma(j)}} \underbrace{(-1)^{\sigma \circ t_{i,j}}}_{= -(-1)^{\sigma}} \underbrace{\operatorname{prod}_{\sigma \circ t_{i,j}} A}_{= \operatorname{prod}_{\sigma} A} + \sum_{\substack{\sigma \in S_n; \\ \sigma(i) > \sigma(j)}} (-1)^{\sigma} \operatorname{prod}_{\sigma} A$$

(since $(-1)^{t_{i,j}} = -1$ and $(-1)^{\sigma\tau} = (-1)^{\sigma}(-1)^{\tau}$)

(since the only factors that differ between $\operatorname{prod}_{\sigma \circ t_{i,j}} A$ and $\operatorname{prod}_{\sigma} A$ are $a_{i, (\sigma \circ t_{i,j})(i)}$ vs. $a_{i, \sigma(i)}$ and $a_{j, (\sigma \circ t_{i,j})(j)}$ vs. $a_{j, \sigma(j)}$; but these factors contribute the same product, because

$$a_{i,(\sigma \circ t_{i,j})(i)} \, a_{j,(\sigma \circ t_{i,j})(j)} = a_{i, \sigma(j)} \, a_{j, \sigma(i)} \overset{(39)}{=} a_{j, \sigma(j)} \, a_{i, \sigma(i)}$$

)

$$= \sum_{\substack{\sigma \in S_n; \\ \sigma(i) > \sigma(j)}} \left(-(-1)^{\sigma}\right) \operatorname{prod}_{\sigma} A + \sum_{\substack{\sigma \in S_n; \\ \sigma(i) > \sigma(j)}} (-1)^{\sigma} \operatorname{prod}_{\sigma} A$$

$$= \sum_{\substack{\sigma \in S_n; \\ \sigma(i) > \sigma(j)}} \underbrace{\left(-(-1)^{\sigma} + (-1)^{\sigma}\right)}_{=0} \operatorname{prod}_{\sigma} A = 0. \qquad \square$$

Example: Let A be a 5×5-matrix of the form

$$\begin{pmatrix} a & b & c & d & e \\ p & 0 & 0 & 0 & f \\ o & 0 & 0 & 0 & g \\ n & 0 & 0 & 0 & h \\ m & l & k & j & i \end{pmatrix}.$$

Then, $\det A = 0$.

([Detnotes, Exercise 6.6(b)].)

Proof. Each $\sigma \in S_5$ satisfies $\operatorname{prod}_{\sigma} A$ (because if $\sigma \in S_5$, then $\sigma(2), \sigma(3), \sigma(4)$ cannot all lie in the set $\{1, 5\}$, so at least one of them lies in $\{2, 3, 4\}$, and thus

contributes a factor of 0 to $\operatorname{prod}_\sigma A$). □

See Spring 2018 Math 4707 HW #4 for two exercises in the same spirit.

See [detnotes, Ch. 6] for (much) more about determinants.

See [Zeilberger, A combinatorial Approach to Matrix Algebra.].

5. Endofunctions

5.1. Basic structure

Def. Let S be a set. An <u>endofunction</u> of S is a map $f: S \to S$.

The <u>cycle digraph</u> of such an f is defined just as for permutations, but no longer needs to consist of cycles.

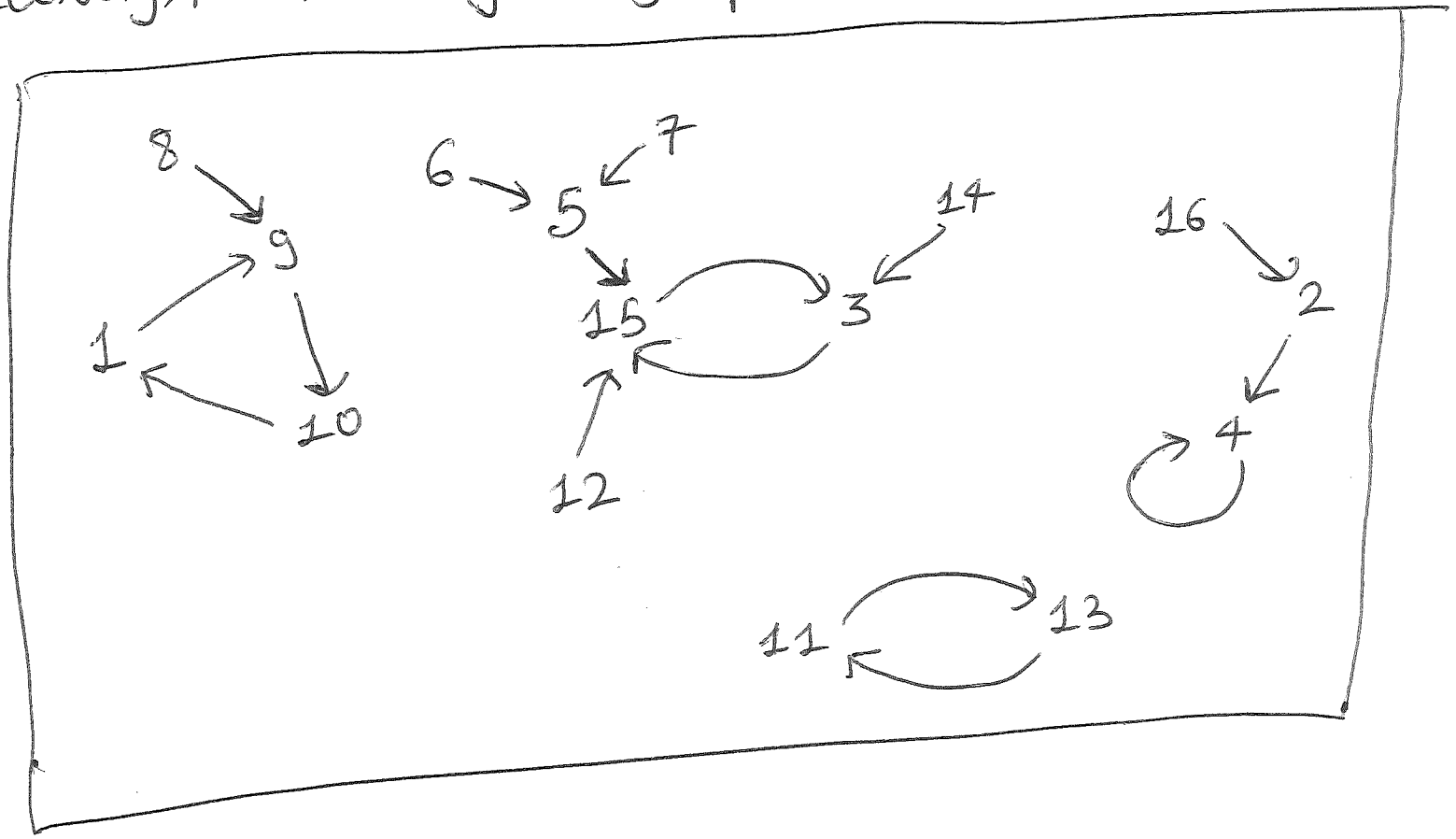
If $S = [n]$, we can define the <u>one-line notation</u> of f as for permutations (i.e., as $(f(1), f(2), \ldots, f(n))$).

Example: Let $S = [16]$. Let f [illegible] $: S \to S$ send

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16

to 9, 4, 15, 4, 15, 5, 5, 9, 10, 1, 13, 15, 11, 3, 3, 2

(respectively). The cycle digraph of f is



Prop. 5.1. Let $n \in \mathbb{N}$. Let S be an n-element set. Let $f : S \to S$ be any map. Write f^k for $\underbrace{f \circ f \circ \cdots \circ f}_{k \text{ times}}$ (whenever $k \in \mathbb{N}$).

(a) We have $f^0(S) \supseteq f^1(S) \supseteq f^2(S) \supseteq \cdots$.

(b) We have $f^n(S) = f^k(S)$ for all $k \geq n$.

(c) The map $f^n(S) \to f^n(S)$, $x \mapsto f(x)$ is well-defined and a permutation of $f^n(S)$.

(d) If $n > 0$, then $f^n(S) = f^{n-1}(S)$.

(e) If $x \in f^n(S)$, then $\exists\, p \in [n]$ such that $x = f^p(x) = f^{2p}(x) = \cdots$. (Such elements x are called recurrent.)

(f) If $x \in S \setminus f^n(S)$, then $f^i(x) \neq x$ $\forall i > 0$. (Such elements x are called transient.)

(g) If $x \in S$, then $\exists\, p \in [n]$ such that $f^p(x) = f^{2p}(x)$.

(h) If $x \in S$ and $q \in \mathbb{N}$, then $\exists\, p \in [n]$ such that $f^p(x) = f^{2p+q}(x)$.

(i) $\exists\, p \in [n^n]$ such that $f^p = f^{2p}$.

Proof. (a) For each $i \in \mathbb{N}$, we have

$$f^{i+1}(S) = f^i(\underbrace{f(S)}_{\subseteq S}) \subseteq f^i(S).$$

(b) If $S = \varnothing$, then this is obvious. $\Rightarrow$ WLOG assume $S \neq \varnothing$.

Then $|f^n(S)| \geq 1$.

Now, the $n+1$ numbers $|f^0(S)|, |f^1(S)|, \ldots, |f^n(S)|$ form a weakly decreasing sequence (by (a)) sandwiched between n and 1:

$$n \geq |f^0(S)| \geq |f^1(S)| \geq |f^2(S)| \geq \cdots \geq |f^n(S)| \geq 1.$$

$\Rightarrow$ By Pigeonhole Princ., two of them are equal.

$\Rightarrow$ $\exists\, q \in [n]$ such that $|f^{q-1}(S)| = |f^q(S)|$.

Consider this q. From $|f^{q-1}(S)| = |f^q(S)|$ and $f^{q-1}(S) \supseteq f^q(S)$, we get $f^{q-1}(S) = f^q(S)$.

$$\xrightarrow{\text{apply } f} f^q(S) = f^{q+1}(S)$$

$$\xrightarrow{\text{apply } f} f^{q+1}(S) = f^{q+2}(S)$$

$$\Longrightarrow \cdots\cdots,$$

Thus, by induction,

(40) $$f^{q-1}(S) = f^k(S) \quad \forall k \geq q-1.$$

Applying this to $k=n$ (since $n \geq q \geq q-1$), we get $f^{q-1}(S) = f^n(S)$. Thus, $f^n(S) = f^{q-1}(S) = f^k(S)$ $\forall k \geq q-1$ and therefore also $\forall k \geq n$. This proves (b).

(d) Apply (40) to $k=n-1$; thus, get $f^{q-1}(S) = f^{n-1}(S)$ (since $\underbrace{n-1}_{\geq q} \geq q-1$). Hence, $f^{n-1}(S) = f^{q-1}(S) = f^n(S)$.

(c) We have $f(f^n(S)) = f^{n+1}(S) \overset{(b)}{=} f^n(S)$.

Thus, the map $f^n(S) \to f^n(S)$, $x \mapsto f(x)$ is well-defined & surjective $\Longrightarrow$ also bijective (by the Pigeonhole Principle for surjections) $\Longrightarrow$ a permutation of $f^n(S)$.

(e) Let $x \in f^n(S)$. Let g be the map from (c).

The $n+1$ elements $g^0(x), g^1(x), \ldots, g^n(x)$ of S cannot all be distinct (since $|S| = n < n+1$). Thus, $\exists$ $0 \leq a < b \leq n$ such

that $g^a(x) = g^\beta(x)$. Consider these a & β.

We have $g^a(x) = g^\beta(x) = g^{a+(\beta-a)}(x) = g^a(g^{\beta-a}(x))$.

But g^a is injective (since g is a permutation), so this yields $x = g^{\beta-a}(x)$. In other words, $x = f^{\beta-a}(x)$ (since $g^i(x) = f^i(x)$ $\forall i \in \mathbb{N}$). Hence,

$$x = f^{\beta-a}(x)$$

$$\xrightarrow{\text{apply } f^{\beta-a}} \quad f^{\beta-a}(x) = f^{2(\beta-a)}(x)$$

$$\xrightarrow{\text{apply } f^{\beta-a}} \quad f^{2(\beta-a)}(x) = f^{3(\beta-a)}(x)$$

$$\Longrightarrow \quad \cdots$$

Thus, by induction, $x = f^{\beta-a}(x) = f^{2(\beta-a)}(x) = \cdots$.

So (e) holds (just take $p = \beta - a$).

(f) Let $x \in S \setminus f^n(S)$, we must prove $f^i(x) \neq x$ $\forall i > 0$.

Assume the contrary. $\Rightarrow$ $\exists\, i > 0$ such that $f^i(x) = x$.

Consider such i.

We have $x = f^i(x) \Rightarrow f^i(x) = f^{2i}(x) \Rightarrow f^{2i}(x) = f^{3i}(x) \Rightarrow \cdots$.

Thus, $x = f^i(x) = f^{2i}(x) = \cdots$.

$\Rightarrow x = f^{ni}(x) \in f^{ni}(S) \subseteq f^n(S)$ (since $ni \geq n$).

This contradicts $x \in S \setminus f^n(S)$. Thus, (f) is proven.

(h) ~~Induction on n.~~ Strong induction on N:

~~Base case: Vacuously true for $n=0$.~~

Step: Fix $N \in \mathbb{N}$. Assume (h) holds when $n < N$.

Now, prove (h) holds when $n = N$.

So let S be an N-element set, and $f: S \to S$, and $x \in S$ and $q \in \mathbb{N}$. Want to find $p \in [N]$ such that $f^p(x) = f^{2p+q}(x)$.

Case 1: $x \in f^N(S)$. (That is, x is recurrent.)

Thus, Prop. 5.1 (e) shows that $\exists\, r \in [N]$ such that $x = f^r(x) = f^{2r}(x) = \cdots$.

Consider this r.

There exists a $p \in [r]$ such that $p+q \equiv 0 \bmod r$.

This p satisfies $f^{p+q}(x) = x$

(since $x = f^r(x) = f^{2r}(x) = \cdots$),

and thus $f^{2p+q}(x) = f^p(\underbrace{f^{p+q}(x)}_{=x}) = f^p(x)$.

So we are done in Case 1, because $p \in [r] \subseteq [N]$

(since $r \in [N]$).

Case 2: $x \notin f^N(S)$. Thus, $x \in S \setminus f^N(S)$.

(That is, x is transient.)

Let $Y = S \setminus \{x\}$. Thus, $|Y| = |S| - 1 = N$.

Prop. 5.1.1(f) yields $f^i(x) \neq x$ $\forall i > 0$.

Thus, the map $Y \to Y$, $y \mapsto f(y)$ is well-defined.

Let $Y = \{f^i(x) \mid i > 0\}$. Then, the map

$g: Y \to Y, \quad y \mapsto f(y)$

is well-defined. Moreover, Prop. 5.1(f) yields $f^i(x) \neq x \ \forall i > 0$. Thus, $x \notin Y$. Hence, $|Y| < |S| = N$. Thus, by the induction hypothesis, we can apply Prop. 5.1(h) to Y, $f(x)$, $q+1$, g instead of S, x, q, f.

We conclude that $\exists\, \tilde{p} \in [|Y|]$ such that $g^{\tilde{p}}(f(x)) = g^{2\tilde{p}+(q+1)}(f(x))$.

Consider this $\tilde{p}$. We have $\tilde{p} \leq |Y| < N$, so $\tilde{p} \leq N-1$, so $\tilde{p}+1 \in [N]$. Also, g is a restriction of f. Thus,

$$g^{\tilde{p}}(f(x)) = g^{2\tilde{p}+(q+1)}(f(x))$$

rewrites as $f^{\tilde{p}}(f(x)) = f^{2\tilde{p}+(q+1)}(f(x))$,

i.e. as $f^{\tilde{p}+1}(x) = f^{2\tilde{p}+q+2}(x)$,

i.e. as $f^{\tilde{p}+1}(x) = f^{2(\tilde{p}+1)+q}(x)$.

Thus, $\exists\ p \in [n]$ such that $f^p(x) = f^{2p+q}(x)$ (namely, $p = \tilde{p}+1$).

This ~~proves~~ completes the induction step.

$\Rightarrow$ Prop. 5.1(h) is proven.

(g) Apply (h) to $q=0$.

(i) WLOG $S = [n]$.

For each $x \in S$, Prop. 5.1(g) shows that $\exists\ p_x \in [n]$ such that $f^{p_x}(x) = f^{2p_x}(x)$. Consider this p_x.

Now, let $p = p_1 p_2 \cdots p_n \in [n^n]$.

Then, $\forall\ x \in S$, we have $f^{p_x}(x) = f^{2p_x}(x)$

$\Rightarrow f^r(x) = f^{2r}(x)$ $\forall$ ~~r~~ r divisible by p_x

$\Rightarrow f^r(x) = f^{2r}(x)$ $\forall\ r$ divisible by p_x.

Apply this to $r = p$ (which is a multiple of each p_x) to

get $f^p(x) = f^{2p}(x) \quad \forall x \in X$.

Thus, $f^p = f^{2p}$. □

Rmk: Prop 5.1 (i) can be strengthened:

$\exists\, p \in [\mathrm{lcm}(1, 2, \ldots, n)]$ such that $f^p = f^{2p}$.