

REU 2005 · Discrete Mathematics · Lecture 1

Lecturer: László Babai
Scribe: Eric Purdy

June 21, 2005. Last updated June 21, 2005

1 Lecture 1

1.1 The Determinant

Let A be an $n \times n$ matrix, $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$. What is the determinant of A ? The algorithm to calculate it using cofactors is not a definition.

Definition 1.1 (Determinant (incomplete)).

$$\det(A) := \sum_{\sigma} \left(\pm \prod_{i=1}^n a_{i\sigma(i)} \right)$$

where σ runs over all permutations of $\{1, \dots, n\}$.

There are $n!$ such permutations, hence this sum has $n!$ terms. But how do we decide whether to choose $+$ or $-$ for each term in this summation?

1.2 Permutations

A permutation on a set X is a function $\sigma : X \rightarrow X$, such that an inverse function σ^{-1} exists.

An example:

| i | i^{σ} |
|-----|--------------|
| 1 | 2 |
| 2 | 3 |
| 3 | 1 |
| 4 | 4 |

We can construct a directed graph to represent a permutation σ , in which there is an edge from i to j if $i^{\sigma} = j$. This is called the permutation graph. Every vertex in this digraph has out-degree 1 and in-degree 1.

Clearly, a permutation graph will be a union of disjoint cycles: if we start at a vertex i and follow the arrows in the digraph, we will eventually come back

to i . If τ is the following permutation

$$\begin{array}{l} i \quad i^\tau \\ 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 4 \\ 4 \mapsto 3 \end{array}$$

then the permutation graph of τ is two cycles of length 2.

1.3 Composing Permutations

When we wish to compose two functions f and g , we write $f \circ g$ to mean the function that results from applying first g , and then f . When we are speaking of permutations, we will reverse this convention. The product $\sigma\tau$ means the permutation that results from applying first σ and then τ . A useful mnemonic is the following: $x^{fg} = (x^f)^g$; first, f is applied to x , and then g .

With σ and τ as defined above, what is $\sigma\tau$?

$$\begin{array}{l} i \quad i^\sigma \quad i^{\sigma\tau} \\ 1 \mapsto 2 \mapsto 1 \\ 2 \mapsto 3 \mapsto 4 \\ 3 \mapsto 1 \mapsto 2 \\ 4 \mapsto 4 \mapsto 3 \end{array}$$

What is the identity element for this operation? It is the identity permutation, which takes i to i for every i . We shall refer to this permutation as id .

What is σ^{-1} ? We need a permutation that satisfies $\sigma\sigma^{-1} = \text{id}$. We can find this by switching the columns in σ , and then rearranging the rows to put them in the correct order.

$$\begin{array}{l} i \quad i^\sigma \quad i \quad i^{\sigma^{-1}} \quad i \quad i^{\sigma^{-1}} \\ 1 \mapsto 2 \quad 2 \mapsto 1 \quad 1 \mapsto 3 \\ 2 \mapsto 3 \quad 3 \mapsto 2 \quad 2 \mapsto 1 \\ 3 \mapsto 1 \quad 1 \mapsto 3 \quad 3 \mapsto 2 \\ 4 \mapsto 4 \quad 4 \mapsto 4 \quad 4 \mapsto 4 \end{array}$$

Alternatively, we can reverse the direction of every arrow in the permutation graph.

S_n is the group of all permutations on $\{1, \dots, n\}$, with multiplication defined as above. S_n is called the *symmetric group* of degree n .

The *order* of a group is the number of elements in the group. The order of S_n is $n!$, the number of permutations on n objects.

Suppose $T \subseteq S_n$. T is said to *generate* the set of permutations $\langle T \rangle = \{\tau_1^{\pm 1}, \tau_2^{\pm 1}, \dots, \tau_k^{\pm 1} \mid \forall i, \tau_i \in T, k \in \mathbb{N}\}$. In English, $\langle T \rangle$ is the set of all products made up of elements from T and their inverses. $\langle T \rangle$ is a *subgroup* of S_n , that is:

1. $\langle T \rangle$ is closed under multiplication: for every $\tau_1, \tau_2 \in \langle T \rangle$, $\tau_1\tau_2 \in \langle T \rangle$.

2. $\langle T \rangle$ is closed under inverses: for every $\tau \in \langle T \rangle$, $\tau^{-1} \in \langle T \rangle$.

3. $\langle T \rangle$ contains the identity (take $k = 0$: the empty product).

1.4 Cycle Notation for Permutations

We use the notation $(3\ 5\ 6)$ to denote the permutation which sends 3 to 5, 5 to 6, and 6 to 3, leaving all other points fixed. Note that this notation is not unique; $(5\ 6\ 3)$ is the same permutation as $(3\ 5\ 6)$.

A cycle of length 2, $(i\ j)$, is called a *transposition*.

Exercise 1.2. *The set of all transpositions generates S_n .*

The expression of a given permutation in terms of transpositions is not unique, but the parity of the number of transpositions is.

Exercise* 1.3. *If $\tau_1\tau_2\cdots\tau_k = \mu_1\mu_2\cdots\mu_\ell$, and the τ_i and the μ_j are transpositions, then $k \equiv \ell \pmod{2}$.*

We call a permutation *even* (*odd*, respectively) if it can be written as the product of an even (odd, respectively) number of permutations. By the above, every permutation is either even or odd, but not both.

We define

$$\text{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}.$$

We can think of sgn as a function from S_n to $\{1, -1\}$.

Exercise 1.4. $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$.

Let A_n be the set of even permutations. A_n is clearly closed under multiplication. Also, $A_n = \text{sgn}^{-1}(1)$. A_n is called the *alternating group* of degree n .

Exercise 1.5. *For $n \geq 2$, $|A_n| = \frac{n!}{2}$.*

The sgn function is what we need to complete the definition of the determinant.

Definition 1.6 (Determinant).

$$\det(A) := \sum_{\sigma \in S_n} \left(\text{sgn}(\sigma) \prod_{i=1}^n a_{i\sigma(i)} \right) \quad (1)$$

1.5 Lattices

Consider \mathbb{Z}^n , the set of n -tuples of integers. $\mathbb{Z}^n = \{(a_1, a_2, \dots, a_n) \mid \forall i, a_i \in \mathbb{Z}\}$
 For $n = 2$, this gives us a grid.

Now, for any two vectors $u, v \in \mathbb{Z}^2$ which are linearly independent, we can define the set $\mathbb{Z}u + \mathbb{Z}v := \{au + bv \mid a, b \in \mathbb{Z}\}$. This set is called a *lattice*.

Pictorially, this gives us a grid of parallelograms which cover the entire plane. Each parallelogram is a shifted copy of the *fundamental parallelogram*

$$P(u, v) = \{au + bv \mid a, b \in \mathbb{R}, 0 \leq a, b \leq 1\}.$$

Exercise 1.7. *The area of the fundamental parallelogram is $\left| \det \begin{pmatrix} u \\ v \end{pmatrix} \right|$*

We can repeat this construction in n dimensions. If u_1, u_2, \dots, u_n are linearly independent vectors in \mathbb{Z}^n , they define a lattice

$$\mathbb{Z}u_1 + \mathbb{Z}u_2 + \dots + \mathbb{Z}u_n = \left\{ \sum_{i=1}^n a_i u_i \mid a_i \in \mathbb{Z} \right\}.$$

In this case, the *fundamental parallelepiped* is the set

$$P(u, v) = \left\{ \sum_{i=1}^n a_i u_i \mid a_i \in \mathbb{R}, 0 \leq a_i \leq 1 \right\}.$$

Exercise 1.8. *The volume of the fundamental parallelepiped of the lattice $\mathbb{Z}u_1 + \mathbb{Z}u_2 + \dots + \mathbb{Z}u_n$ is*

$$\left| \det \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \right|.$$

Use only the following two properties of volume in \mathbb{R}^n :

- The volume of a brick with side-lengths a_i is $\prod_{i=1}^n a_i$.
- If you cut up and rearrange pieces of a set, the volume will remain the same.

1.6 Polynomials

A *polynomial* is an expression of the form $f(x) = \sum_{i=1}^n a_i x^i$. The *degree* of a polynomial is the index of the highest non-zero coefficient, i.e., $\deg(f) = \max\{j \mid a_j \neq 0\}$. $a_j x^j$ is called the *leading term* of f .

Since all the coefficients of the zero polynomial are zero, this definition does not give us a value for $\deg(0)$. We shall adopt the convention that $\deg(0) = -\infty$.

Corollary 1.9. $\deg(fg) = \deg(f) + \deg(g)$

Corollary 1.10. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$

Exercise 1.11. If $\deg(f) \neq \deg(g)$, then $\deg(f + g) = \max\{\deg(f), \deg(g)\}$.

\mathbb{Q} is the set of rational numbers. $\mathbb{Q}[x]$ is the set of polynomials over \mathbb{Q} , i. e., polynomials with rational coefficients.

Definition 1.12. f is irreducible if $\deg(f) \geq 1$ and $f = gh \implies \deg(g) = 0$ or $\deg(h) = 0$, i. e., either g or h is a nonzero constant.

The last chapter of the “Algebra Review” handout has information and exercises relating to irreducible polynomials.

Theorem 1.13 (Gauss’s Lemma). Let $f \in \mathbb{Z}[x]$. Suppose $f = gh$, where $g, h \in \mathbb{Q}[x]$. Then there exists $r \in \mathbb{Q}$, $r \neq 0$, with $rg \in \mathbb{Z}[x]$ and $\frac{1}{r}h \in \mathbb{Z}[x]$. $f = gh = (rg)(\frac{1}{r}h)$. Therefore, if f can be factored in $\mathbb{Q}[x]$, f can also be factored in $\mathbb{Z}[x]$.

If we are trying to factor an integer polynomial, Gauss’s Lemma dramatically reduces the number of possible factors. This means that we can factor many more integer polynomials by hand.

Exercise 1.14. Factor $x^4 + 4$.

1.7 Semigroups

Notation 1.15. $(\exists!x)$ is read as “there exists a unique x such that”

A *semigroup* is a set S together with a binary operation $*$, such that the following axioms hold:

1. $(\forall a, b \in S)(\exists!a * b \in S)$
2. $*$ is associative: $(\forall a, b, c \in S)(a * (b * c) = (a * b) * c)$.

Note that we do not require that $*$ is commutative!

Notation 1.16. $\mathbb{N} = \{0, 1, \dots\}$.

Example 1.17. $(\mathbb{N}, +)$ is a semigroup. (\mathbb{N}, \cdot) is also a semigroup.

Example 1.18. $5 + \mathbb{N} = \{5, 6, \dots\}$. $(5 + \mathbb{N}, +)$ is a semigroup. $(5 + \mathbb{N}, \cdot)$ is also a semigroup.

Example 1.19. The set of $n \times n$ matrices, together with the operation \cdot , is an example of a noncommutative semigroup.

Any group is also a semigroup.

Definition 1.20. e is a right identity in S if $(\forall x \in S)(xe = x)$. A left identity is defined analogously.

Lemma 1.21. *If a semigroup S has a right identity e , and a left identity f , then both are unique, and $e = f$.*

Proof. $e = fe = f$. □

Definition 1.22. z is a left zero in S if $(\forall x \in S)(zx = z)$. A right zero is defined analogously.

Exercise 1.23. *If a semigroup S has a right zero z , and a left zero y , then both are unique, and $z = y$.*

Example 1.24 (Left-zero Semigroup). *For any set S , we can define a semigroup with the following operation: $x * y = x$. This is called the left-zero semigroup on S . Every element of S is a left zero. This semigroup is not commutative for $|S| \geq 2$.*

If every element of a semigroup is a right identity, then every element is also a left zero, and vice versa.

Definition 1.25. a is an idempotent in S if $a^2 = a$.

Example 1.26. $(\mathbb{N} + 5, +)$ is a semigroup with no idempotents.

Exercise 1.27. *If S is a finite, nonempty semigroup, then S has an idempotent.*

Definition 1.28. An idempotent semigroup is a semigroup in which each element is an idempotent.

Example 1.29. *The left-zero semigroup on any set S is idempotent.*

Definition 1.30. A semilattice is a commutative idempotent semigroup.

This concept is not related to the lattices discussed earlier.

Example 1.31. *Let (\mathbb{Z}, \max) is a semilattice.*

Example 1.32. *Let A be a set, and let 2^A be the power set of A , i. e., the set of all subsets of A . Then $(2^A, \cup)$ and $(2^A, \cap)$ are semigroups. Both of these semigroups are semilattices.*

Definition 1.33. A subsemigroup T of a semigroup S is a subset of S which is closed under the operation. We write $T \leq S$ to denote this.

Example 1.34. *For every $a, b \in \mathbb{N}$, the following are subsemigroups of $(\mathbb{N}, +)$: $\mathbb{N} + b$, $a\mathbb{N}$, $a\mathbb{N} + ab$, and $a\mathbb{N} + b\mathbb{N}$.*

Exercise 1.35. *If $T \leq (\mathbb{N}, +)$, then $\exists k$ such that $T \subseteq k\mathbb{N}$ and $k\mathbb{N} \setminus T$ is finite. In other words, all subsemigroups of $(\mathbb{N}, +)$ are “ultimately periodic.”*

Exercise 1.36. *Find two infinite sets $A, B \subseteq \mathbb{N}$ such that*

$(\forall z \in \mathbb{N})(\exists! a \in A, b \in B)(z = a + b)$.

In other words, every nonnegative integer z can be uniquely written as the sum of a member of A and a member of B .

(Comment: If we did not require A and B both to be infinite, the following would be a simple example: $A = \{0, 1, 2, 3, 4, 5, 6\}$, $B = 7\mathbb{N}$.)