

Linear Algebra, 3rd day, Wednesday 6/30/04
REU 2004. Info:
<http://people.cs.uchicago.edu/~laci/reu04>.

Instructor: László Babai
Scribe: Richard Cudney

1 Rank

Let V be a vector space.

Definition 3.1. Let $S \subseteq V$, and $T \subseteq S$. T is a set of **generators** of S if $S \subseteq \text{Span}(T)$.

Definition 3.2. A **basis** of S is a linearly independent set of generators of S .

Definition 3.3. The **rank** of a set S , $\text{rk}(S) := |B|$ for any basis B of S . Note that this is well-defined because of the Fundamental Fact.

Definition 3.4. Let $U \leq V$. The **dimension** of U , $\dim(U) := \text{rk}(U)$ (=maximal number of linearly independent vectors in U).

Exercise 3.5. $\dim \text{Span}(T) = \text{rk}(T)$ Hint: One direction is immediate and the other follows from the fundamental fact.

Given a matrix, there are a priori two different ranks associated to it, the rank of the set of column vectors, and the rank of the set of row vectors (column-rank and row-rank respectively). It is an Amazing Fact that row-rank=column-rank. The following exercise gives a proof of this fact using Gaussian elimination.

- Exercise 3.6.**
- (a) Elementary row operations **change** which **sets** of rows are linearly independent, while the maximum number of linearly independent rows remains the same.
 - (b) Elementary column operations do not affect the linear independence of any given set of rows.
 - (c) By applying elementary row and column operations any matrix can be made to have zeroes everywhere outside a square sub-matrix in the upper left hand corner, in which it will have ones down the diagonal and zero elsewhere.

Exercise 3.7 (Rank invariance under field extensions). If \mathbb{F}, G are fields, $\mathbb{F} \leq G$ and A is a matrix over \mathbb{F} , then $\text{rk}_{\mathbb{F}}(A) = \text{rk}_G(A)$.

2 Number Fields, Roots of Unity

Exercise 3.8. If \mathbb{F} is a number field then $\mathbb{F} \supseteq \mathbb{Q}$.

Recall the previous exercise that asked to show that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a number field. The only non-obvious part was that we could divide by non-zero elements. We can accomplish division by multiplying by the conjugate:

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

Exercise 3.9. Let $a, b \in \mathbb{Q}$. If $a^2 - 2b^2 = 0$ then $a = b = 0$.

Now how can we generalize this trick to show that $\mathbb{Q}[\sqrt[3]{2}]$ is a number field? What are the conjugates of $\sqrt[3]{2}$? Previously we used both roots of $x^2 - 2$, now we want to use all roots of $x^3 - 2$. What are the other roots beside $\sqrt[3]{2}$? Let $\omega = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$ so that $\omega^2 = \cos(\frac{4\pi}{3}) + i\sin(\frac{4\pi}{3})$. These are the non-real roots of $x^3 = 1$, so $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ are the other cube roots of 2.

Note:

$$\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

and

$$\omega^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

This example leads us to study the n -th roots of unity-the complex solutions of

$$x^n = 1.$$

We can calculate the n -th roots as follows, writing x in polar form:

$$x = r(\cos(\alpha) + i\sin(\alpha))$$

$$x^n = r^n(\cos(n\alpha) + i\sin(n\alpha)) = 1 + i0$$

So $r = 1$, and $\alpha = \frac{2k\pi}{n}$.

Exercise 3.10. Let S_n be the sum of all n th roots of unity. Show that $S_0 = 1$ and $S_n = 0$ for $n \geq 1$.

Definition 3.11. z is a **primitive** n -th root of unity if $z^n = 1$ and $z^j \neq 1$ for $1 \leq j \leq n - 1$.

Let

$$\zeta_n := \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right) = e^{2\pi i/n}$$

Exercise 3.12. $1, \zeta_n, \dots, \zeta_n^{n-1}$ are all of the n -th roots of unity.

Exercise 3.13. Let $z^n = 1$. Then the powers of z give all n -th roots of unity iff z is a primitive n -th root of unity.

Exercise 3.14. Suppose z is a primitive n -th root of unity. For what k is z^k also a primitive n -th root of unity?

Exercise 3.15. If z is an n -th root of unity then z^k is also an n -th root of unity.

Definition 3.16. The **order** of a complex number is the smallest positive n such that $z^n = 1$. (If no such n exists then we say z has infinite order.)

$$\text{ord}(-1) = 2, \text{ord}(\omega) = 3, \text{ord}(i) = 4, \text{ord}(1) = 1, \text{ord}(\pi) = \infty.$$

Exercise 3.17. $\text{ord}(z) = n$ iff z is a primitive n -th root of unity.

Exercise 3.18. Let $\mu(n)$ be the sum of all primitive n -th roots of unity.

- a) Prove that for every n , $\mu(n) = 0, 1$, or -1 .
- b) Prove $\mu(n) \neq 0$ iff n is square free.
- c) Prove if $\text{g.c.d.}(k, \ell) = 1$ then $\mu(k\ell) = \mu(k)\mu(\ell)$.
- d) If $n = p_1^{t_1} \dots p_k^{t_k}$, find an explicit formula for $\mu(n)$ in terms of the t_i .

Exercise 3.19. Show that the number of primitive n -th roots of unity is equal to Euler's phi function. $\varphi(n) :=$ number of k such that $1 \leq k \leq n$, $\text{g.c.d.}(k, n) = 1$.

n	$\varphi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

Definition 3.20. $f : \mathbb{N}^+ \rightarrow \mathbb{C}$ is **multiplicative** if $(\forall k, \ell)(\text{g.c.d.}(k, \ell) = 1 \text{ then } f(k\ell) = f(k)f(\ell))$.

Definition 3.21. f is **totally multiplicative** if $(\forall k, \ell)(f(k\ell) = f(k)f(\ell))$.

Exercise 3.22. μ function is multiplicative.

Exercise 3.23. φ function is multiplicative.

Exercise 3.24. Neither μ nor φ are totally multiplicative.

Exercise 3.25. Prove that
$$\sum_{d|n, 1 \leq d \leq n} \varphi(d) = n.$$

Remark 3.26. We call

$$g(n) = \sum_{d|n, 1 \leq d \leq n} f(d)$$

the **summation function** of f .

Exercise 3.27. f is multiplicative if and only if g is.

Now, using the preceding ideas, we can apply in $\mathbb{Q}[\sqrt[3]{2}]$ the same construction we used in $\mathbb{Q}[\sqrt{2}]$:

$$\frac{1}{a + \sqrt[3]{2}b + \sqrt[3]{4}c} \cdot \frac{a + \omega \sqrt[3]{2}b + \omega^2 \sqrt[3]{4}c}{a + \omega \sqrt[3]{2}b + \omega^2 \sqrt[3]{4}c} \cdot \frac{a + \omega^2 \sqrt[3]{2}b + \omega \sqrt[3]{4}c}{a + \omega^2 \sqrt[3]{2}b + \omega \sqrt[3]{4}c}.$$

Exercise 3.28. Show that the denominator in the above expression is rational and non-zero.

3 Irreducible Polynomials

Definition 3.29. Let \mathbb{F} be a number field. $\mathbb{F}[x]$ is the ring of all univariate polynomials with coefficients in \mathbb{F} .

Definition 3.30. f is **irreducible** over \mathbb{F} if

- (i) $\deg(f) \geq 1$ and
- (ii) $(\forall g, h) (\in \mathbb{F}[x], f = gh \rightarrow \deg(f) = 0 \text{ or } \deg(g) = 0)$.

Remark 3.31. If $\deg(f) = 1$, then f is irreducible because degree is additive.

Theorem 3.32 (Fundamental Theorem of Algebra). *If $f \in \mathbb{C}[x]$ and $\deg(f) \geq 1$ then $(\exists \alpha \in \mathbb{C})(f(\alpha) = 0)$.*

Exercise 3.33. Over \mathbb{C} a polynomial is irreducible iff it is of degree 1. HINT: Follows from the FTA and the exercise ?? that lets you pull out roots.

Definition 3.34. Let $f, g \in \mathbb{F}[x]$. We say $f | g$ if $(\exists h)(fh = g)$.

Exercise 3.35. $(\forall \alpha)(x - \alpha) | (f(x) - f(\alpha))$.

Corollary 3.36. α is a root of f iff $(x - \alpha) \mid f(x)$.

Remark 3.37. If $f(x) = x^n$, then

$$x^n - \alpha^n = (x - \alpha)(x^{n-1} + \alpha x^{n-2} + \dots + \alpha^{n-1}).$$

Exercise 3.38. $f(x) = ax^2 + bx + c$ is irreducible over \mathbb{R} iff $b^2 - 4ac < 0$.

Remark 3.39. Odd degree polynomials over \mathbb{R} always have real roots.

Exercise 3.40. If $f \in \mathbb{R}[x]$, and $z \in \mathbb{C}$, then $f(\bar{z}) = \overline{f(z)}$.

Consequence: If z is a root of f then so is \bar{z} .

Theorem 3.41. Over \mathbb{R} , all irreducible polynomials have $\deg \leq 2$.

Proof: Suppose $f \in \mathbb{R}[x]$, $\deg(f) \geq 3$. We want to show that f is not irreducible over \mathbb{R} .

- 1) If f has a real root α , then $(x - \alpha) \mid f$.
- 2) Otherwise by FTA f has a complex root z which is not real, so that $z \neq \bar{z}$. Thus $(x - z)(x - \bar{z}) = x^2 - 2ax + a^2 + b^2$ divides f , where $z = a + bi$.

□

Theorem 3.42 (Gauss Lemma). If $f = gh$, $f \in \mathbb{Z}[x]$, $g, h \in \mathbb{Q}[x]$ then $\exists \alpha \in \mathbb{Q}$ such that $\alpha g \in \mathbb{Z}[x]$ and $\frac{h}{\alpha} \in \mathbb{Z}[x]$.

Exercise 3.43. If a_1, \dots, a_n are distinct integers, then $\prod_{i=1}^{i=n} (x - a_i) - 1$ is irreducible over \mathbb{Q} .

Exercise 3.44. $\forall n, x^n - 2$ is irreducible over \mathbb{Q} .

Definition 3.45. The n -th **cyclotomic polynomial** is $\Phi_n(x) = \prod (x - \zeta)$, where ζ ranges over the primitive n -th roots of unity.

Remark 3.46. $\deg \Phi_n(x) = \varphi(n)$.

$$\begin{aligned} \Phi_1(x) &= x - 1 \\ \Phi_2(x) &= x + 1 \\ \Phi_3(x) &= x^2 + x + 1 \\ \Phi_4(x) &= x^2 + 1 \\ \Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\ \Phi_6(x) &= x^2 - x + 1 \\ \Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ \Phi_8(x) &= x^4 + 1 \end{aligned}$$

Exercise 3.47. $x^n - 1 = \prod_{d|n, 1 \leq d \leq n} \Phi_d(x)$.

Exercise 3.48. $\Phi_n(x) \in \mathbb{Z}[x]$.

Theorem 3.49. * $\Phi_n(x)$ is irreducible over \mathbb{Q} .

Definition 3.50. $\alpha \in \mathbb{C}$ is **algebraic** if $(\exists f)(f \in \mathbb{Q}[x], f \neq 0, f(\alpha) = 0)$.

Definition 3.51. A **minimal polynomial** for α is a nonzero polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ such that

$$m_\alpha(\alpha) = 0 \tag{1}$$

and $m_\alpha(x)$ has minimal degree, among polynomials satisfying (??).

Remark 3.52. The minimal polynomial is well-defined up to a constant multiple.

Exercise 3.53. $m_\alpha(x)$ is irreducible.

Definition 3.54. $\deg(\alpha) = \deg(m_\alpha)$.

Exercise 3.55. If ζ is a primitive n th root of unity then $\deg(\zeta) = \varphi(n)$.

Exercise 3.56. $(\forall f \in \mathbb{Q}[x])(f(\alpha) = 0 \iff m_\alpha \mid f)$

Definition 3.57. The **algebraic conjugates** of α are the roots of m_α .

Exercise 3.58. If $\deg(\alpha) = n$ then the set

$$\mathbb{Q}[a] := \{a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Q}\}$$

is a field.