Math 296 (the Linear Algebra parts[1])

Atharva Gawde

February 23, 2024

[1]I didn't lock in before this.

Contents

Lecture 1

Vector Spaces

1.1 Recall from last class:

Example. We showed that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

Proof. We have two cases

(i) If n is primes we use Bezout's lemma to find inverses.

(ii) If n is composite, we get zero-divisors.

1.2 Ring Homomorphism

Lemma 1. Let F be a field. Then there exists a unique $\varphi\colon \mathbb{Z} \to F$ such that for all $n, m \in \mathbb{Z}$

(i) $\varphi(1) = 1_F$

(ii) $\varphi(n + m) = \varphi(n) +_F \varphi(m)$

(iii) $\varphi(n \cdot m) = \varphi(n) \cdot_F \varphi(m)$

Proof. We can construct φ from these properties... $\square$

Note. A function $\varphi\colon \mathbb{Z} \to \mathbb{F}$ (or from any ring) that satisfies (i), (ii), and (iii) is called a ring homomorphism.

Lemma 2. Let F be a field, Let $\varphi\colon \mathbb{Z} \to F$ be the ring homomorphism we just defined. Then either

(i) $\ker(\varphi) = \{0\}$ if and only if φ is injective, or

(ii) $\ker(\varphi) = p\mathbb{Z}$ for some prime p.

Proof. If φ is injective... $\square$

1.3 Characteristic

Definition 1. Let F be field. Let $\varphi\colon \mathbb{Z} \to F$ be the unique ring homomorphism. If φ is injective, then we say that F has characteristic 0. If φ is not injective, then we say F has characteristic p, where $\ker(\varphi) = p\mathbb{Z}$.

Example. $\operatorname{char}(\mathbb{C}) = 0$

Example. $\operatorname{char}(\mathbb{R}) = 0$

Example. $\operatorname{char}(\mathbb{Z}/67\mathbb{Z}) = 67$

Lemma 3. Suppose F is a finite field, then $\varphi\colon \mathbb{Z} \to F$ can not be injective, so F has prime characteristic.

Lemma 4. If F has characteristic p, then $\underbrace{1_F + \cdots + 1_F}_{p \text{ times}} = 0$ and if $\underbrace{1_F + \cdots + 1_F}_{n \text{ times}} = 0$ then $p \mid n$.

1.4 Polynomials

Definition 2. A polynomial over a finite field F is a formal expression of the form $a_n x^n + \cdots a_1 x + a_0$ where $n \in \mathbb{N} \cup \{0\}$ and $a_i \in F$ for all $0 \leq i \leq n$, and x is a formal variable.

Note. This is not a function like in 295.

Definition 3. The 0 polynomial is called the trivial polynomial.

Definition 4. A nontrivial polynomial can be written as $b(x) = b_0 + b_1 x + \cdots + b_\ell x^\ell$ with $b_\ell \neq 0$, we say b has degree ℓ.

Lecture 5

Algebraic Numbers

5.1 Algebraic Numbers

Definition 5. Fix $\alpha \in \mathbb{C}$. Define $\mathbb{Q}[\alpha] = \operatorname{span}(\alpha^i \mid i \in \mathbb{N} \cup \{0\})$ monomial powers of α. This is vector space over $\mathbb{Q}$.

Definition 6. The element $\alpha \in \mathbb{C}$ is algebraic provided that there exists a nonzero polynomial $p \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$.

Example. $\alpha = \sqrt{2}$ is algebraic with $p(x) = x^2 - 2$.

Example. $i \in \mathbb{C}$ is algebraic with $p(x) = x^2 + 1$.

Example. $\pi \in \mathbb{C}$ is not algebraic.

Definition 7. If $\alpha \in \mathbb{C}$ is not algebraic, then α is called transcendental.

Example. $\pi \in \mathbb{C}$ is transcendental.

Lemma 5. Let $\alpha \in \mathbb{C}$. Then $\mathbb{Q}[\alpha]$ is finitely generated over $\mathbb{Q}$ if and only if α is algebraic.

Proof. Suppose $\mathbb{Q}[\alpha]$ is finitely generated. Then there exists scalars $\overline{v_1}, \overline{v_2}, \ldots, \overline{v_m} \in \mathbb{Q}[\alpha]$ such that $\mathbb{Q}[x] = \operatorname{span}(\overline{v_1}, \overline{v_2}, \ldots, \overline{v_m})$. For each $1 \leq i \leq m$ we know $\overline{v_i} \in \mathbb{Q}[\alpha]$ so we can write

$$\overline{v_i} = q_{i_0} + q_{i_1}\alpha^1 + \cdots + q_{i_{n_1}}\alpha^{n_i}$$

where we can assume $q_{i_{n_i}} \neq 0$. To avoid this hellish notation let's replace this with

$$\begin{aligned} \overline{v_1} &= \text{mess}_1 \quad \deg n_1 \\ \overline{v_2} &= \text{mess}_2 \quad \deg n_2 \\ &\vdots \\ \overline{v_m} &= \text{mess}_m \quad \deg n_m. \end{aligned}$$

Let $M = \max\{n_1, \dots, n_m\}$. Since $\alpha^{M+1} \in \mathbb{Q}[\alpha]$ there exist scalars $d_1, \dots, d_m \in \mathbb{Q}$ such that $\alpha^{M+1} = d_1\overline{v_1} + \cdots + d_m\overline{v_m}$. Then $\alpha^{M+1} = d_1(\text{mess}_1) + \cdots + d_m(\text{mess}_m) = r_0 + r_1\alpha^1 + \cdots + r_M\alpha^M$ with $r_i \in \mathbb{Q}$ by expanding all messes and collecting like terms in powers of α. Define $p(x) = x^{M+1} - (r_0 + r_1x^1 + \cdots + r_Mx^M)$. We can clear the denominators to get a nonzero polynomial $\widetilde{p}(x) \in \mathbb{Z}[x]$ such that $\widetilde{p}(\alpha) = 0$, so α is algebraic. $\square$

Note. This is only one direction of this proof, we will prove the other direction next time.

Recall from last time:

Lemma 6. Let $\alpha \in \mathbb{C}$. Then the vector space $\mathbb{Q}[\alpha] := \text{span}_{\mathbb{Q}}(1, \alpha, \alpha^2, \dots)$ is finitely generated over $\mathbb{Q}$ if and only if $\alpha \in \overline{\mathbb{Q}}$

Proof. Last time we showed the forward direction. We assumed $\mathbb{Q}[\alpha]$ is finitely generated and we found a nonzero polynomial $\widetilde{p} \in \mathbb{Z}[x]$ such that $\widetilde{p}(\alpha) = 0$. We took a generating family $(\overline{v_1}, \dots, \overline{v_m})$, and for all $1 \le i \le m$, there exist scalars in $\mathbb{Q}$ such that $\overline{v_i} = \underbrace{q_{i_0} + q_{i_1}\alpha^1 + \cdots + q_{i_{n_1}}\alpha^{n_i}}_{\text{mess}_i}$. Let $M = \max\{n_1, n_2, \dots, n_m\}$. Consider $\alpha^{M+1} \in \mathbb{Q}[\alpha]$. There exist scalars $d_1, \dots, d_m \in \mathbb{Q}$ such that

$$\begin{aligned} \alpha^{M+1} = \alpha^{M+1} &= d_1\overline{v_1} + \cdots + d_m\overline{v_m} \\ &= d_1(\text{mess}_1) + \cdots + d_m(\text{mess}_m) \\ &= r_0 + r_1\alpha^1 + \cdots + r_M\alpha^M \end{aligned}$$

So $0 = -\alpha^{M+1} + r_0 + r_1\alpha^1 + \cdots + r_M\alpha^M$. So defined $p(x) = -x^{M+1} + r_0 + r_1x^1 + \cdots + r_Mx^M$ and we multiplied out the denominators to get $\widetilde{p} \in \mathbb{Z}[x]$.

Now we need to prove the other direction, assume $\alpha \in \overline{\mathbb{Q}}$. We will begin with a motivating example.

Example. Suppose α is a root of $x^5 - 67x^2 + 3 = 0$, how does this give us a generating family for $\mathbb{Q}[x]$?

Let's continue with the proof. Since $\alpha \in \overline{\mathbb{Q}}$ there exist a nonzero $p \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$. We can write $p(\alpha) = a_0 + a_1\alpha^1 + \cdots a_N\alpha^N$ with $a_i \in \mathbb{Z}$ and $a_N \neq 0$. So

$$\alpha^N = -\frac{a_0}{a_N} - \frac{a_1}{a_N}\alpha^1 - \cdots - \frac{a_{N-1}}{a_N}\alpha^{N-1} \qquad (*)$$

We claim $\underbrace{\mathbb{Q}[x]}_{\text{LHS}} = \underbrace{\text{span}(1, \alpha, \ldots, \alpha^{N-1})}_{\text{RHS}}$. We will show this by two-way containment. We have LHS $\supseteq$ RHS immediately from definitions. To show LHS $\subseteq$ RHS, fix $\overline{v} \in$ LHS so $\overline{v} = \sum_{i \in \mathbb{N} \cup \{0\}} b_i\alpha^i$ with $b_i \in \mathbb{Q}$ and all but finitely many are zero.

Define the degree of $\overline{v}$ to be $\max\{i \in \mathbb{N} \cup \{0\} \mid b_i \neq 0\}$, that is the greatest nonzero power. Note this is empty if $\overline{v} = \overline{0}_V$. In this case $\overline{v} \in$ RHS so we are done. Assume $\overline{v} \neq \overline{0}_V$ so a maximum exists.

We start with a nice case, if $\deg(\overline{v}) < N$, we are done. Now let's tackle a harder case. For $\deg(\overline{v}) \geq N$ set $j = \deg(\overline{v}) - (N-1)$. Note $j = 1$ when $\deg(\overline{v}) = N$. We will induct on j. So for our base case $j = 1$, we have $deg(\overline{v}) = N$. We want to show $\overline{v} \in$ RHS. By $(*)$, we may replace α^N in $\overline{v}$ with the combination in $(*)$. Then $\overline{v}$ is a linear combination of vectors in $(1, \alpha, \alpha^2, \ldots, \alpha^{N-1})$ so we win!

Now we have our strong inductive hypothesis: Suppose that if $1 \leq j < n$, then $\overline{v} \in$ RHS. We will prove that if $j = n$, then $\overline{v} \in$ RHS. Assume $j = n$, so $\deg(\overline{v}) - (N-1) = n$, or alternatively, $\deg(\overline{v}) = n + (N-1)$. So we can write $\overline{v}$ as

$$\begin{aligned}\overline{v} &= b_{N-1+n}\alpha^{N-1+n} + \overline{v}' \\ &= b_{N-1+n} \cdot \alpha^{n-1} \cdot \alpha^N + \overline{v}'\end{aligned}$$

with $b_{N-1+n} \in \mathbb{Q} \setminus \{0\}$ and $\deg(\overline{v}') < N - 1 + n$. Now we can replace α^N with $(*)$ so

$$\overline{v} = b_{N-1+n}\left[-\frac{a_0}{a_N} - \frac{a_1}{a_N}\alpha^1 - \cdots - \frac{a_{N-1}}{a_N}\alpha^{N-1}\right] + \overline{v}'$$

and by our inductive hypothesis $\overline{v} \in$ RHS. $\square$