Lecture 2

Fields and Polynomials

2.1 Recall from last class

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

Explanation. We have two cases.

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

(ii) If n is composite, we get zero-divisors. That is, if n is composite, there exist a, b with $2 \leq a \leq b \leq n-1$ such that $n = ab$. So then we have $ab \equiv 0 \mod n$ so a and b form a pair of zero divisors; that is, nonzero elements in $\mathbb{Z}/n\mathbb{Z}$ whose product is 0.

> **Note.** This contradiction arises from something we proved in 295. If F is a field and $a, b \in F$ such that $ab = 0$, then either $a = 0$ or $b = 0$. In other words, a field can not have zero divisors.

2.2 Ring Homomorphisms

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) $\varphi(n+m) = \varphi(n) +_F \varphi(m)$, that is φ is a group homomorphism with respect to $+$

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

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

Proof. We can construct φ from these properties, building it from the ground up. To satisfy (i), we define $\varphi(i) := 1_F$. Then by (ii), we have $\varphi(2) := \varphi(1+1) = \varphi(1) +_F \varphi(1) = 1_F +_F +1_F$. Naturally, $\varphi(3) :=$

$1_F +_F 1_F +_F 1_F$ and so forth. So we define

$$\varphi(n) := \underbrace{1_F +_f \cdots +_F 1_F}_{n \text{ times}}.$$

We have that (1) and (2) hold by construction, and by some casework we have $\varphi(\underbrace{1 + \cdots + 1}_{n \cdot m \text{ times}}) = \underbrace{1_F +_F \cdots +_F 1_F}_{n \cdot m \text{ times}} = \varphi(n) \cdot_F \varphi(m)$, satisfying (3). This construction is unique since it was completely determined by (1) and (2), and we got (3) as a consequence of using the ring $\mathbb{Z}$, we can take this as a definition. $\square$

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, then $\ker(\varphi) = \{0\}$ (by homework). Suppose φ is not injective. Then there exists $n \in \mathbb{N}$ such that $\ker(\varphi) = n\mathbb{Z}$. Write $n = ab$ for some integers a, b such that $1 \leq a \leq b \leq n$, so $\varphi(n) = \varphi(a) \cdot_F \varphi(b)$. That is we have $0_F = \varphi(a) \cdot_F \varphi(b)$ so $\varphi(a) = 0$ or $\varphi(b) = 0$ without loss of generality. $\square$

2.3 Characteristic

Definition 1 (Characteristic)**.** Let F be a 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. $\operatorname{char}(\mathbb{Z}/67\mathbb{Z}) = 67$

Example. There are examples of infinite fields that have prime characteristic. Let's start with $F_p = \mathbb{Z}/p\mathbb{Z}$. Then we have the ring

$$F_p[x] := \{\text{polynomials with coefficients in } \mathbb{Z}/p\mathbb{Z} \text{ with variable } x\}$$

Here are some definitions and theorems that are literally only for the purpose of this example.

Definition 2 (Integral Domain [Hungerford]). A commutative ring R with identity $1_R \neq 0$ and no zero divisors is called an integral domain.

Definition 3 ([Hungerford]). A nonempty subset S of a ring R is multiplicative provided that $a, b \in S$ implies $ab \in S$.

Theorem 1 ([Hungerford]). Let S be a multiplicative subset of a commutative ring R. The relation defined on the set $R \times S$ by

$$(r, s) \sim (r', s') \text{ if and only if } s_i(rs' - r's) = 0 \text{ for some } s \in S$$

is an equivalence relation. Furthermore if R has no zero divisors and $0 \notin S$, then

$$(r, s) \sim (r', s') \text{ if and only if } rs' - r's = 0.$$

Proof. You do it. Not me. Or see Hungerford Chapter III Theorem 4.2. This is not really not part of this class. I will not do it. □

Theorem 2 ([Hungerford]). Denote the equivalence class $(r, s) \in R \times S$ by r/s. Let $S^{-1}R$ be the set of all equivalence classes of $R \times S$ under the equivalence relation $\sim$ above.

(i) $S^{-1}R$ is a commutative ring with identity, where addition and multiplication are defined by

$$r/s + r'/s' = (rs' + r's)/ss' \text{ and } (r/s)(r'/s') = rr'/ss'.$$

(ii) If R is a nonzero ring with no zero divisors and $0 \in S$, then $S^{-1}R$ is an integral domain.

(iii) If R is a nonzero ring with no zero divisors and S is the set of all nonzero elements of R, then $S^{-1}R$ is a field.

Proof. You do this one too. Not me. Or see Hungerford Chapter III Theorem 4.3. This is still not part of this class. □

Definition 4 (Ring of Quotients [Hungerford]). The ring $S^{-1}R$ is called the ring of quotients (often ring of fractions or quotient ring) of R by S. In the case where S is the set of all nonzero elements in an integral domain R, then $S^{-1}R$ is a field called the quotient field (often field of fractions) of the integral domain R.

Let $R(x)$ be the quotient field of $R[x]$. To make this more understandable,

$$R(x) = \{p/q \mid p \in R[x], q \in R[x] \setminus \{0\}\}.$$

This is an infinite field. So $F_p(x)$ is an infinite field with characteristic p.

Explanation. It is up to you to prove all the assumptions above. That is, you should prove that the polynomials in one variable over a field form a ring, and further, an integral domain. You should verify the aforementioned theorems. You should prove that the characteristic of $F_p(x)$ is p. It really is not part of this class. It is just a good example. I will not do it. I will not do it. I will not do it.

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 $p \mid n$.

2.4 Polynomials

Definition 5 (Polynomial)**.** 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 6. The set of all polynomials with coefficients in F is denoted $F[x]$.

Definition 7. The 0 polynomial is called the trivial polynomial.

Definition 8 (Degree of a Polynomial)**.** A nontrivial polynomial can be written as $b(x) = b_0 + b_1 x + \cdots + b_\ell x^\ell$ with $b_\ell \neq 0$. In this case, we say b has degree ℓ.

> **Remark.** What should the degree of the trivial polynomial be? Some say -1. Others $-\infty$ to heuristically satisfy that for all $p, q \in F[x]$
>
> $$\deg(p \cdot q) = \deg(p) + \deg(q)$$

Definition 9 (Polynomial Function)**.** A polynomial function is a function $F \to F$ that can be defined by evaluating a polynomial in $F[x]$.

Example. To make the distinction between polynomials and polynomial functions clear, consider $f, g\colon \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ where $f(x) = x^3 + x$ and $g(x) = 2x$. These are different polynomials, but the same function.

Lemma 5. If $p, q \in F[x]$ and $c \in F$, then

(i) $p + q \in F[x]$

(ii) $p \cdot q \in F[x]$

(iii) $c \cdot p \in F[x]$.

Lemma 6 (Descartes). Let $\alpha \in F$ and let $p \in F[x]$ be nonzero. Then $p(\alpha) = 0$ if and only if there exists $q \in F[x]$ with $\deg(p) = \deg(q) + 1$ such that $p(x) = (x - \alpha)q(x)$.

Proof. The backwards implication is immediate from evaluating the expression. For the forward implication, since p is nonzero and $p(\alpha) = 0$ we must have $\deg(p) \geq 1$. Write $p(x) = c_m x^m + \cdots + c_1 x + c_0$ with $c_i \in F$. Then $p(\alpha) = c_m \alpha^m + \cdots + c_1 \alpha + c_0$. So we have $p(x) = p(x) - 0 = p(x) - p(\alpha) = c_m(x^m - \alpha^m) + \cdots c_1(x - \alpha)$. Then from homework this is $= (x - \alpha) \underbrace{\sum_{i=1}^{m} c_i G_{i-1}(\alpha, x)}_{q(x)}$ where we apply $x^i - \alpha^i = (x - \alpha) \cdot G_{i-1}(x, \alpha)$ where $G_n(\alpha, x) = \sum_{k=0}^{n} x^n \alpha^{n-k}$ to each term and factor out $(x - \alpha)$, leaving us with $q(x)$ with $\deg(q) = m - 1$. □

Definition 10 (Root of a Polynomial). Let $p \in F[x]$ be nonzero. The field element $\alpha \in F$ is called a root or a zero of p provided that $p(\alpha) = 0$.

Corollary. Let $p \in F[x]$ be nonzero. Then p has $\leq \deg(p)$ roots in F.

Proof. Note that the statement holds if $\deg(p) = 0$. We will use induction on $\deg(p)$. Let our candidate inductive set be $S := \{n \in \mathbb{N} \mid$ if $q \in F[x]$ is nonzero and has $\deg(q) \leq n$, then q has $\leq \deg(q)$ roots$\}$. We have that $1 \in S$, since polynomials of degree one are of the form $q(x) = ax + b$ with $a, b \in F$ and $a \neq 0$, so we can just solve for the root. Suppose $k \in S$ and let $q \in F[x]$ be nonzero with degree $k + 1$. If q has no roots we are done. If q does have a root, we can use Descartes to write $q(x) = (x - \alpha) \cdot r(x)$ where $\deg(r) = \deg(q) - 1 = k$, and so our statement holds by the inductive hypothesis and $k + 1 \in S$. □

Lingo. A field F is *algebraically closed* provided that every nonconstant polynomial in $F[x]$ has a root.

Remark. $\mathbb{C}$ is algebraically closed by the Fundamental Theorem of Algebra. We can build the closure of any field by "throwing in the roots", like $\overline{\mathbb{Q}}$.

Example. Is $\mathbb{Z}/2\mathbb{Z}$ algebraically closed? No, we have that $x, x+1, x-1, x^2+1, x^2-1$ all have roots, but x^2+x+1 has no root in $\mathbb{Z}/2\mathbb{Z}$. What does $\overline{\mathbb{Z}/2\mathbb{Z}}$, the smallest algebraically closed field containing $\mathbb{Z}/2\mathbb{Z}$ look like?

Lecture 3

Vector Spaces

3.1 Recall from last class

Last time we explored $F[x]$, the ring of polynomials over a field F. We arrived at some interesting results about their roots, specifically

Lemma 7 (Descartes)**.** Let $\alpha \in F$ and let $p \in F[x]$ be nonzero. Then $p(\alpha) = 0$ if and only if there exists $q \in F[x]$ with $\deg(q) = \deg(p) - 1$ such that $p(x) = (x - \alpha)q(x)$.

Corollary (still ask sarah, can't we just take $q = 1$, what are we really saying here?)**.** Let $p \in F[x]$ be nonzero. Suppose $\alpha_1, \ldots, \alpha_k \in F$ are roots of p. Then

(i) There exists $q \in F[x]$ such that $q(\alpha_i) \neq 0$ for all $1 \leq i \leq k$, and

(ii) There exist $m_1, \ldots, m_k \in \mathbb{N}$ such that $p = (x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} \cdots (x - \alpha_k)^{m_k} \cdot q$.

> **Remark.** m_i is called the multiplicity of α_i.

Fun Fact. Let F be a finite field with characteristic p. Then $|F| = p^n$.

3.2 Vectors and Vector Spaces

What is a vector? A quantity? A scalar? Something with magnituede and direction? Starts at the origin? - 296ers.

Definition 11 (Vector)**.** A vector $\overline{v}$ is an element of a vector space.

Definition 12 (Vector Space)**.** Let F be a field (often called the field of scalars or the ground field). A vector space over the field F is a set V equipped with two operations

(i) $+$ from $: V \times V \to V$ called vector addition

(ii) $\cdot$ from $: F \times V \to V$ called scalar multiplication

such that

(i) $(V, +)$ is an abelian group. So $+$ is commutative and associative, there exists a unique identity element $\overline{0} \in V$, and we have unique additive inverses.

(ii) For all $c \in F$ for all $\overline{v}_1, \overline{v}_2 \in V$, we have $c \cdot (\overline{v}_1 + \overline{v}_2) = c \cdot \overline{v}_1 + c \cdot \overline{v}_2$

(iii) For all $c_1, c_2 \in F$ for all $\overline{v} \in V$, we have $(c_1 + c_2) \cdot \overline{v} = c_1 \cdot \overline{v} + c_2 \cdot \overline{v}$.

(iv) For all $c_1, c_2 \in F$ for all $\overline{v} \in V$, we have $(c_1 c_2) \cdot \overline{v} = c_1 \cdot (c_2 \cdot \overline{v})$.

(v) For all $\overline{v} \in V$, we have $1_F \cdot \overline{v} = \overline{v}$.

Example. $V = \mathbb{R}^n$ is a vector space over $F = \mathbb{R}$ where $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$ defines vector addition, and for all $c \in \mathbb{R}$, scalar multiplication is defined as $c \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} cx_1 \\ \vdots \\ cx_n \end{pmatrix}$.

Example. $V = \mathbb{C}^n$ is a vector space over $F = \mathbb{R}$.

Question. Given a field F, is F a vector space over itself?

Explanation. Yes TODOTODOTODOTODO