Lec 9/8

Friday, September 8, 2017 14:15

$a_n \nearrow \infty$

Can $\alpha_0 + \alpha_1 a_1 + \alpha_2 a_2 + \cdots$ represent any number (where $0 \le \alpha_i < a_i$)

Beta expansion of $x \in \mathbb{R}$

$x = \sum \frac{b_i}{\beta^i}$ where $1 < \beta \in \mathbb{R}$

Reading: Rest of Ch 7, Ch 8 120-126

All finite fields are known

for any $p \in P$, $n \in \mathbb{N}$, $\exists$ a unique field having p^n elements (up to isomorphism)

Facts: ① each finite field has $\mathbb{Z}_p$ as a subfield

$\exists p \in P$ s.t. $\sum_{i=1}^{p} 1 = 0$. $F \ni 1$, $\underbrace{1+1+\cdots+1}_{k \text{ times}} \in F$ $k \le p-1$, $\sum_{i=1}^{k} 1$

sequence $1, 1+1, \ldots, 1+\cdots+1$

exists smallest n s.t. $\underbrace{1+\cdots+1}_{n} = 0$ (pigeonhole principle)

n is prime. If not, $n = n_1 n_2$ but $\underbrace{(1+\cdots+1)}_{n_1}\underbrace{(1+\cdots+1)}_{n_2} \neq 0$

since n is minimal.

② If $|F| < \infty$ then $\exists p \in P$, $n \in \mathbb{N}$ s.t. $|F| = p^n$.

If F is a field and F_0 is a subfield,

then F is a v.space over F_0.

q.

Then F is v.space over $\mathbb{Z}_p$.

If V/F, $\dim V = d$, then $V \approx F^d = \{(a_1, \dots, a_d);\ a_i \in F\}$

$F \cong \mathbb{Z}_p^d$ since F finite $\Rightarrow$ $\dim F = d$ finite.

(3) $\forall p \in P\ \exists F$ w/ $|F| = p^2$.

Exercise field w/ p^2 elements. How many automorphisms does it have?

Exercise Let G be a cyclic group $\{e, a, a^2, \dots, a^{k-1}\}$, $|G| = k$.
What is the cardinality of $\mathrm{Aut}(G)$? (perhaps $\phi(k)$)

Exercise Show there is a fieldof a field of p^3 elements

Fact in any finite field (in particular $\mathbb{Z}_p$), the multiplicative group is cyclic.

Exercise if G is a group and $|G| = p$ then g is cyclic

$\mathbb{Z}_m$ is a field iff $m \in P$.

if $m \notin P$, $m = n_1 n_2$, so $n_1 n_2 \equiv 0 \mod m$.

Q: What are invertible elements in $\mathbb{Z}_m$? how many are there?

Important fields:

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (and finite fields in general),

rational functions: $\left\{ \frac{f(x)}{g(x)} ;\ f, g \in \mathbb{R}[x] \right\}$,

Algebraic numbers, $\mathbb{Q}[\lambda]$, $\lambda \in \mathbb{R}$.

google: Integral Domain
Ex: $\mathbb{Z}$, $\mathbb{R}[x]$, etc.

Algebraic numbers, $\mathbb{Q}[\lambda]$, $\lambda \in \mathbb{R}$.

Do the solutions of integer quadratic eqns form a field?

Do constructible numbers form a field? If so, is it countable?

p-adic numbers

Noncommutative field of importance: $\mathbb{H}$ (quaternions)

$$\left\{ a + bi + cj + dk, \quad a, b, c, d \in \mathbb{R} \right.$$

$$\begin{tikzcd} & i \arrow[dr] & \\ k \arrow[ur] & & j \arrow[ll] \end{tikzcd} \qquad \left. i^2 = j^2 = k^2 = -1 \right\}$$

Exercise $\mathbb{H}$ is isomorphic to $\left\{ \begin{pmatrix} u & -v \\ \bar{v} & \bar{u} \end{pmatrix} ; \ u, v \in \mathbb{C} \right\}$

There are no 3-dimensional complex numbers

Theorem $\forall\, a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \ \exists\, x_1, x_2, x_3, x_4$ s.t.

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

(if $a_i, b_i \in \mathbb{Z}$ then $x_i \in \mathbb{Z}$)

Proof: $\det \begin{pmatrix} u & -v \\ \bar{v} & \bar{u} \end{pmatrix} = u\bar{u} + v\bar{v} =$ four squares.

$$(a_1^2 + 2a_2^2)(b_1^2 + 2b_2^2) = x_1^2 + 2x_2^2$$

$$\det \begin{pmatrix} a_1 & -2a_2 \\ a_2 & a_1 \end{pmatrix}$$

(Weyl, 1916) a sequence x_n is uniformly distributed (in $[0,1]$) if

(Weyl, 1916) a sequence x_n is uniformly distributed (in $[0,1]$) if

$\forall \; 0 \le a < b \le 1$ we have $\lim_{N \to \infty} \frac{\#\{1 \le n \le N : x_n \in (a,b)\}}{N} = b - a$

exercise prove this one → $n\alpha \bmod 1$, $n^2\alpha \bmod 1$, $n^3\alpha \bmod 1$, $\log^{\epsilon+1} n \bmod 1$

are all uniformly distributed.

Exercise create a natural rational sequence which is uniformly distributed.