Last time: Classifying quadratic sp / $\mathbb{C}$, $\mathbb{R}$

Now: $\mathbb{F}_p$

Prop $\mathbb{F}_p^\times$ is cyclic (works for any finite field not just $\mathbb{F}_p$)

Pf sk let $G = \mathbb{F}_p^\times$ → G is abelian of order $p-1$

Def $G[n] = \{g \in G \mid g^n = 1\}$ is a subgp of G.

Claim $\#G[n] \leq n$

$x \in G[n] \Rightarrow x^n = 1 \Rightarrow x^n - 1 = 0$

$\Rightarrow x$ is a root of $T^n - 1$

General fact → over any field, a poly of degree n has at most n roots (by division)

General fact if G is finite abelian with $\#G[n] \leq n$ $\forall n$

$\Rightarrow G$ is cyclic

prove using structure thm of fin abelian grp → **Main**

$\hookrightarrow G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ s.t. $n_1 \mid n_2 \mid \cdots \mid n_r$

Cor if p is odd $\mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2$ has order 2

Pf $G = \mathbb{F}_p^\times$ is a cyclic grp of even order

$\cong \mathbb{Z}/(p-1)\mathbb{Z}$

In other words, (p odd) $\exists$ some elt $\varepsilon \in \mathbb{F}_p^\times$ that is not a square & $\mathbb{F}_p^\times = \mathbb{F}_p^\times \sqcup \varepsilon \mathbb{F}_p^\times$ → for $\mathbb{R}$ $\varepsilon = -1$

for $\mathbb{Z}/\text{odd}\,\mathbb{Z}$

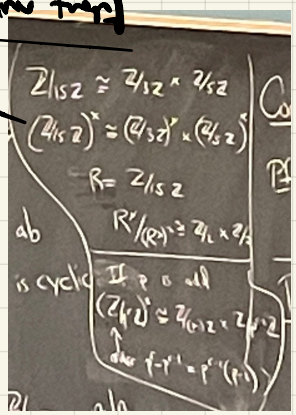
Prop Every elt of $\mathbb{F}_p$ is a sum of 2 squares! → p odd

Lemma let k be a field (not char 2)

$S_2 = \{x \in k^\times \mid \exists a, b \in k \text{ s.t. } x = a^2 + b^2\}$

Then S_2 is a subgp of $k^\times$

ring of rational integers



Pf) Say $a+ib$, $c+id \in \mathbb{C}$

know $|(a+ib)(c+id)| = |a+ib| \cdot |c+id|$

$$(ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2)$$

↳ holds as poly in abcd ↳ true in any ring

↳ ⟹ S_2 closed under mult!

for inv consider $\left| \frac{1}{a+bi} \right|$

Rmk) $S_n \subseteq k^\times$

↳ sum of n squares.

$S_1 \to$ gp of sq $\subseteq k^\times$ → subgrp

$S_2 \to$ subgrp of $k^\times$ just shown

In fact, S_n subgrp when $n = 2^r$

↳ theory of Pfister forms.

Pf of prop) note $(\mathbb{F}_p^\times)^2 < S_2 < \mathbb{F}_p^\times$

index 2

It follows $S_2 = \mathbb{F}_p^\times$ or $(\mathbb{F}_p^\times)^2$

If $S_2 = \mathbb{F}_p^\times$ then done. Sppse $S_2 = (\mathbb{F}_p^\times)^2$

(⟹ $\{a^2 \mid a \in \mathbb{F}_p\}$ are an additive subgrp

⟹ any elt of $\mathbb{F}_p$ is a sqr X.

Quad sp / $\mathbb{F}_p$ → p odd & fin dim nondeg

First observation, every quad sp. / $\mathbb{F}_p$ is isom to

$[\underbrace{1, \dots 1}_{r}, \underbrace{\varepsilon, \dots, \varepsilon}_{s}]$ ε is non-square

→ r, s not unique

Lemma) $[\varepsilon, \varepsilon] \cong [1, 1]$ → altir can't have notion of proof. neg def

V: v_1, v_2 W: v_1, v_2 by prop $\varepsilon = a^2 + b^2 \in \mathbb{F}_p$

→

Put $u_1 = a w_1 + b w_2$ $\quad \langle u_1, u_1 \rangle = \varepsilon$

Let u_2' be non-zero orth to u_1.

→ [note: u_1, u_2' form basis of W] → orth ⇒ linind in this case

→ $\langle u_1, u_1 \rangle$ is not isotropic

→ things in span u_1 are not orthogonal

$c = \langle u_2', u_2' \rangle$

In u_1, u_2' basis W has matrix

$\begin{bmatrix} \varepsilon & 0 \\ 0 & c \end{bmatrix}$ → claim $c \in \varepsilon \cdot (\mathbb{F}_p^\times)^2$

initial matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ same Δ

$\Rightarrow \det I = \boxed{\text{Square}} \cdot \det \begin{bmatrix} \varepsilon & 0 \\ 0 & c \end{bmatrix}$

$1 = \boxed{\text{Square}} \cdot \varepsilon \cdot c$ ← $\boxed{\text{nonzero}}$

$\Rightarrow \varepsilon \cdot c \in (\mathbb{F}_p^\times)^2$

$\Rightarrow c = \varepsilon \delta^2$ for $\delta \in \mathbb{F}_p^\times$

Let $u_2 = \frac{u_2'}{\delta}$ $\Rightarrow \langle u_2, u_2 \rangle = \varepsilon$ & $\langle u_1, u_2 \rangle = 0$

Using basis u_1, u_2 get $\begin{bmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{bmatrix}$

get iso

$V \longrightarrow V$

$v_1 \longmapsto u_1$

$v_2 \longmapsto u_2$

D

If V quad sp $[\underbrace{1, \dots, 1}_{r}, \underbrace{\varepsilon, \dots, \varepsilon}_{s}]$

lemma says $V = [\overbrace{1, \dots, 1}^{s+r}]$ if s is even

$V = [\underbrace{1, \dots, 1}_{s+t-1}, \varepsilon]$ if s is odd

Thm If V non-degen n-dim'l quad sp $/\mathbb{F}_p$ then V is isom to

$[1, \dots, 1]$ or $[1, \dots, 1, \varepsilon]$

Also: these 2 sp are not isom!

(b/c disc diff in $\mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2$)

Cor Up to isomorphism, there are 3 anisotropic $/\mathbb{F}_p$

$[1]$, $[\varepsilon]$, $[1, -\varepsilon]$