Lec 19 2/24/2021

- Finite Fields
- Thm of primitive element.

Lemma. Let G be a finite Abelian gp. $|G| = n$. Suppose for each $d \mid n$
$|\{x \in G \mid x^d = 1\}| \leq d$.
Then G is cyclic.

Pf. Let $a_1, \dots, a_m$ be the invariant factors of G.

So $G \cong \mathbb{Z}/(a_1) \oplus \dots \oplus \mathbb{Z}/(a_m)$.

$a_1 \mid a_2 \dots \mid a_m$.

If $m \geq 2$

$x = (0, 0, \dots, 0, \bar{b}, \bar{c})$

then $a_m \cdot x = 0$

And there are $(a_{m-1})(a_m)$ such elements. So there are $> a_m$ elements of order dividing a_m, a contradiction.

So $m = 1$ and G is cyclic.

__Cor.__ Let G be a finite subgroup of $\underline{F}^\times$ for a field F.

Then G is cyclic.

__Pf.__ If $x \in F$ with $x^d = 1$ then x is a root of $x^d - 1 \in F[x]$ so there are at most d such.

So G has $\leq d$ elements of order dividing d, so G is cyclic by the lemma.

__Rmk.__ If F is a finite field, $F^\times$ is cyclic.

Thm. Fix prime $p > 0$. Let F be a finite field with $\operatorname{char} F = p$. Then $|F| = p^n$ some $n \geq 1$, and F is isomorphic to the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

Conversely, for any $n \geq 1$ the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ is a field of p^n elements.

Pf. Consider F = splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Let E = the set of roots of $f = x^{p^n} - x$ in F. $(x^{p^n} - x)' = p^n x^{p^n - 1} - 1 = -1$ so $\gcd(f, f') = 1$, so f is separable and has p^n roots in F.

Then E is a subfield of F:

$\alpha \in E \iff \alpha^{p^n} = \alpha$.

then if $\alpha, \beta \in E$, $(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} = \alpha - \beta$.

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta.$$

$$(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$$

But F = generated over $\mathbb{F}_p$ by the roots in E. So $E = F$. So $|F| = p^n$.

Conversely, let F be any finite

field of char $F = p$. Then
F contains a copy of $\mathbb{F}_p$
= cyclic subgroup under + gen. by 1
then $[F : \mathbb{F}_p] = n \geq 1$ and
$|F| = p^n$, the # of element of
any v.s. of dim n over $\mathbb{F}_p$.
Look at $F^\times$ where $|F^\times| = p^n - 1$.
For $a \in F^\times$, $a^{(p^n-1)} = 1$
So $a^{p^n} = a$ (holds also for $a = 0$)
So $a^{p^n} = a$ for all $a \in F$.
So F consists of the roots of
$x^{p^n} - x \in \mathbb{F}_p[x]$. So F is
a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

Since all splitting fields of $x^{p^n} - x$
over $\mathbb{F}_p$ are isomorphic,
there is only one field of order p^n

up to $\cong$.

<u>Cor.</u> For each $n \geq 1$ there is a irr. polynomial f of degree n in $\mathbb{F}_p[x]$. and $\mathbb{F}_p[x]/(f)$ is a field with p^n elements

<u>Pf.</u> Let $|F| = p^n$, where F is a finite field. $F^\times$ is cyclic, say $F^\times = \langle \gamma \rangle$. Then $\mathbb{F}_p(\gamma) = F$

So $[F : \mathbb{F}_p] = n = \deg \operatorname{minpoly}_{\mathbb{F}_p}(\gamma)$.

So $f = \operatorname{minpoly}_{\mathbb{F}_p}(\gamma)$ is irreducible of deg n.

<u>Ex.</u> x^3+x+1 is irr. in $\mathbb{F}_3[x]$.

Then $F = \mathbb{F}_3[x]/(x^3+2x+1)$ has 27 element.

$$F = \{ \underline{a_0} + \underline{a_1} x + \underline{a_2} x^2 + (\underline{x^3+2x+1}) \}.$$

e.g. $(x + (x^3+2x+1))^{-1} = ?$

$$x(a_0 + a_1 x + a_2 x^2)$$

$$a_0 x + a_1 x^2 + a_2 x^3$$

$$x^3 = -2x - 1$$
$$= x + 2$$

$$a_0 x + a_1 x^2 + a_2 (x+2)$$

$$2a_2 + (a_0 + a_2) x + a_1 x^2 = 1$$

$$2a_2 = 1$$
$$a_0 + a_2 = 0$$
$$a_1 = 0.$$

$$a_2 = 2$$
$$a_0 = 1$$

$$1 + 2x^2$$

Thm (primitive element).

Let $F \subseteq K$ with $[K:F] < \infty$.

TFAE:

① $K = F(\gamma)$ some $\gamma \in K$.

"γ is a primitive element".

② There are finitely many subfields E with

$$F \subseteq E \subseteq K$$

"intermediate fields".

Pf. If $|F| < \infty$, then $|K| < \infty$ so $K^\times$ is cyclic, say $K^\times = \langle \gamma \rangle$ as a group. Then $F(\gamma) = K$.

Condition ② also is automatic since K has finitely many subsets

Now assume $|F| = \infty$.

Let $K = F(\gamma)$ for $\gamma \in K$.

Let $F \subseteq \underline{E} \subseteq K$ and let

$f = \text{minpoly}_{\underline{E}}(\gamma) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$
$\in E[x]$.

Let $E' = F(a_0, \dots, a_{n-1}) \subseteq E \subseteq K$.

$f \in E'[x]$, and so f is also irreducible in $E'[x]$, so

$f = \text{minpoly}_{E'}(\gamma)$.

$[K : E] = [E(\gamma) : E] = \deg f$

$= [E'(\gamma) : E'] = [K : E']$

so $[E : E'] = 1$, so $E = E'$!

Finally if $\underline{g} = \text{minpoly}_F(\gamma)$

then $\text{minpoly}_{\underline{E}}(\gamma)$ divides g in $K[x]$.

But g has finitely many distinct monic factors.

So there are finitely many E's.

Conversely, if there are finitely many intermediate fields E, show if $\alpha, \beta \in K$ then $F(\alpha, \beta) = F(\gamma)$ for some γ. Then since $K = F(\alpha_1, \ldots, \alpha_m)$ some α_i, we get by induction $K = F(\gamma)$ some γ.

idea: look at elements $\alpha + \lambda\beta$ $\lambda \in F$ use $|F| = \infty$. $\gamma = \alpha + \lambda\beta$ some λ.

OUT OF TIME! But full details in course notes. (only a few more steps...)