Math 491 , Tuesday, April 14, Finite Fields

Thu - 22 (Sage)

Fri - 23 (RQ)
w/ WF, CR/NC

Mon - Problem Session
Sage 22

Theorem F finite field $\Rightarrow F^*$ is cyclic (multiplicatively)

Proof F^* finite abelian group, of order $p^n - 1$

then $F^* \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$ (p_i not necessarily unique)

There is an element in F^* w/ a generator of cyclic group,

$g = (g_1, g_2, \dots, g_k)$ $\quad |g_i| = p_i^{n_i}$

$|g| = \operatorname{lcm}(p_1^{n_1}, p_2^{n_2}, \dots, p_k^{n_k}) = m$

Order of <u>any</u> element in F^* will divide m

So every element of F^* is a root of $x^m - 1$,

and $x^m - 1$ has at most m roots $\wedge \Rightarrow |F^*| \leq m$

<u>poly over a field</u>

Also

$$m = \operatorname{lcm}(p_1^{n_1}, p_2^{n_2}, \dots, p_k^{n_k}) \leq p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = |F^*|$$

So $m = |F^*|$ & thus g <u>is</u> a generator of F^*, so F^* cyclic.

Ex $x^{12}+x^6+x^5+x^4+x^2+2 \in \mathbb{Z}_3[x]$ irreducible (Sage)

Let a be a root, form degree 12 extension $\mathbb{Z}_3(a)$

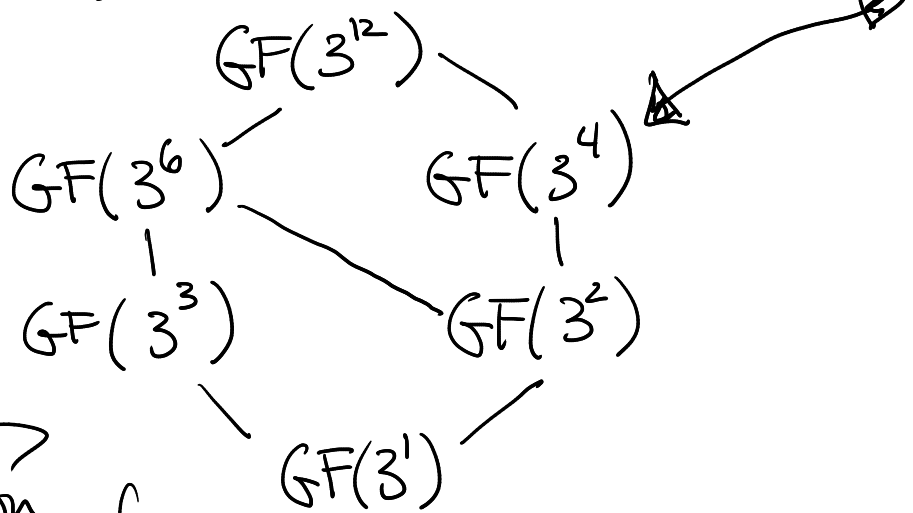
(rewriting rule: $a^{12} = 2a^6+2a^5+2a^4+2a^2+1$)

$[\mathbb{Z}_3(a) : \mathbb{Z}_3] = 12 \Rightarrow \mathbb{Z}_3(a)$ is a finite field of order 3^{12}.

($\mathbb{Z}_3(a)/\mathbb{Z}_3$ vector space w/ basis $\{1, a, a^2, \ldots, a^{11}\}$)

$\mathbb{Z}_3(a) = GF(3^{12})$

Subfields? $GF(p^m)$ where $m \mid 12$



depends on factorization of 12.

$|GF(3^{12})^*| = 3^{12}-1 = 531,440$

$|GF(3^4)^*| = 3^4-1 = 80$

Yesterdays: $80 \mid 531,440$ (because $4 \mid 12$)

$GF(3^{12})^* = \langle a \rangle$ $|a| = 531,440$

$GF(3^4)^*$ subgroup of cyclic group

$GF(3^4)^* = \langle a^? \rangle = \langle a^{\frac{3^{12}-1}{3^4-1}} \rangle = \langle a^{6643} \rangle$ has order 3^4-1

$a^{6643} = a^{10}+2a^9+2a^8+a^7+a^6+2a^4+2a^2+a$