cyclotomic PhL 1.25.13

This has been added into Galois doc at the end of Ch 5.

Consider this conjugate set

$$\{ \alpha, \alpha^{p}, \alpha^{p^2}, \alpha^{p^3} \quad , ... \alpha^{p^{m-1}} \} \qquad \alpha^{p^m} = \alpha^{q} = \alpha \qquad \text{m elements} \qquad (5.14)$$

If we compute these sets for every α^{s}, we get these sets (α = primitive so we hit all q-1 nz elements)

$$\{ \alpha^{s}, \alpha^{sp}, \alpha^{sp^2}, \alpha^{sp^3} \quad , ... \alpha^{sp^{m-1}} \} \qquad \text{s ranges from 1 to q-1 since } \alpha^{s} \text{ are generators}$$

Next element in this set *would* be

$$\alpha^{sp^m} = \alpha^{s} \qquad \text{which follows from } \alpha^{p^m} = \alpha$$

but this is the first element, and that is why we don't include it. It is already included.

In terms of the exponents only, somehow we would say that sp^m and s are equivalent.

Consider the set of exponents of the conjugates

$$C_s \equiv \{ s, sp, sp^2, sp^3, ... sp^{m-1} \}$$

This thing is called a "cyclotomic coset mod p".

How can this equivalence be stated in terms of the mod function?

I think my original hit is just plain wrong. Here is something better

Definition: *Cyclotomic coset* mod p: $C_s = (s, ps, p^2s, ...p^{m-1}s)$
Note that $|C_s|$ is either m or a (nontrivial) divisor of m.

Example: p=2, m=4

$C_0 = \{0\}$ $\quad m_0 = x + 1$
$C_1 = \{1, 2, 4, 8\}$ $\quad m_1 = x^4 + x + 1 = m_2 = m_4 = m_8$
$C_3 = \{3, 6, 9, 12\}$ $\quad m_3 = x^4 + x^3 + x^2 + x + 1 = m_6 = m_9 = m_{12}$
$C_5 = \{5, 10\}$ $\quad m_5 = x^2 + x + 1 = m_{10}$
$C_7 = \{7, 11, 13, 14\}$ $\quad m_7 = x^4 + x^3 + 1 = m_{11} = m_{13} = m_{14}$

$m_0 m_1 m_3 m_5 m_7 = x^{15} + 1$ *over* $\mathbb{F}_2$
$x^{p^m - 1} - 1 = \prod_{b \in \mathbb{F}_{p^m}^\times} (x - b)$ *over* $\mathbb{F}_p$

Definition: The smallest entries of the cyclotomic cosets are called *coset representatives*.
The set of coset representatives in our running example: {0,1,3,5,7}

You can write this as

sq = s //equivalent

This would be true in mod q-1 math ?

k 0,1,2,3,4,5,6,7,8
n 0,1,2,3,0,1,2,3,0 8 = 4 = 0 s4 = 4 n = k mod 4

The exponents in this set are

{ s, sp, sp^2, sp^3, ... sp^{m-1}} // next one would be sp^m which is somehow equivalent to s

This looks close to what my PDF discusses. If I let r = m-1 then this set is

{ s, sp, sp^2, sp^3, ... sp^r}

I just said that s lies in 1 to q-1 which also agrees with my PDF. Now can I show that

sp^{r+1} = s mod(q-1) ?

sp^m = s mod(q-1) ?