HW 10 (Yay!)

① (a) By the Fact, $\deg \Phi_p(x) = \phi(p) = p-1$. Therefore

$$\Phi_p(x) = \frac{x^p - 1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

Over $\mathbb{F}_p$, $x^p - 1 = x^p - 1^p = (x-1)^p$

$$\Rightarrow \Phi_p(x) \bmod p = \frac{x^p-1}{x-1} = \frac{(x-1)^p}{x-1} = (x-1)^{p-1}$$

(b) The # roots of $x^{p^n} - 1 = 0$ of order d inside $\mathbb{F}_{p^n}^\times$ is at most $\phi(d)$. But for each $d \mid p^n - 1$, there are at least $\phi(d)$ roots inside $\mathbb{F}_{p^n}^\times$ since $\mathbb{F}_{p^n}^\times$ contains all the distinct p^n-th roots of unity for each $d \mid p^n - 1$.

$\left(\text{since } |\mathbb{F}_{p^n}^\times| = \sum_{d \mid p^n - 1} \phi(d) \right)$.

(c) $\mathbb{F}_{p^n}^\times$ is cyclic, ie $\mathbb{F}_{p^n}^\times \cong C_{p^n - 1}$. Let α be a generator.
Then $\psi \in \mathrm{Aut}(C_{p^n-1}, C_{p^n-1})$ is determined by $\psi(\alpha)$, which must be a generator. There are $\phi(p^n - 1)$ generators of C_{p^n-1}.

③

(a) Suppose $d \mid n$. Then $n = qd$ so

$$x^n - 1 = x^{qd} - 1 = (x^d)^q - 1 = (x^d - 1)(x^{d(q-1)} + x^{d(q-2)} + \dots)$$

$\Rightarrow x^d - 1 \mid x^n - 1$.

Now suppose $d \nmid n$. If $d > n \Rightarrow$ clearly $x^d - 1 \nmid x^n - 1$.

So assume $d < n$, and write $n = qd + r$ where $q > 0$, $0 < r < d$.

Then $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$

$$= x^r \underbrace{\left(x^{qd} - 1\right)}_{\substack{\text{divisible by} \\ x^d - 1}} + x^r - 1$$

$\Longrightarrow x^d - 1 \mid x^r - 1$ ↯.

(b) If $d \mid n$, then by (a), $a^d - 1 \mid a^n - 1$.

If $d \nmid n$, then by the proof of (a), we must have $a^d - 1 \mid a^r - 1$.

But either $a = 1$ ($0 \mid 0$) or $a \geq 2$, in which case

$2^d - 1 > 2^r - 1$. ↯.

(c) Set $a = p$ now.

If $d \mid n$, then $x^d - 1 \mid x^n - 1$ so the field of dth roots of unity is contained in the field of nth roots of unity.

Conversely, if $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$, then for a generator α of $\mathbb{F}_{p^d}^\times$,

$|\alpha| = p^d - 1 \mid |\mathbb{F}_{p^n}^\times| = p^n - 1$.

④

(a) $f(x) = x^8 - x = x(x^7-1) = x(x-1)\,\Phi_7(x)$.

$\mathrm{Gal}(f(x)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong C_6$.

(b) $f(x) = x^8 - x = x^{2^3} - x \in \mathbb{F}_2[x]$

Splitting field of $f(x)$ is $\cong \mathbb{F}_{2^4} = \mathbb{F}_8$,

$\mathrm{Gal}(f(x)/\mathbb{F}_2) \cong \mathbb{Z}/3\mathbb{Z}$.

(c) $f(x) = x^4 - 1 \in \mathbb{F}_7[x]$.

$= (x-1)\underbrace{(x^3+x^2+x+1)}_{g(x)}$.

$g(-1) = -1+1-1+1 = 0 \Rightarrow (x+1)$ is a root.

$g(x) = x^2(x+1) + (x+1) = \underbrace{(x^2+1)}_{h(x)}(x+1)$.

$h(x) = x^2+1 = x^2-6$ note $-1=6$ is not a square mod 7:

$1^2 = 1,\ 2^2 = 4,\ 3^2 = 2$ (the rest are $-1, -2, -3$)

$\Rightarrow h(x)$ is irred over $\mathbb{F}_7$, degree 2.

$\Rightarrow \mathrm{Gal}(f(x)/\mathbb{F}_7) = \mathrm{Gal}(h(x)/\mathbb{F}_7) \cong C_2$ (only group of order 2)

(5) Let $\alpha = \sqrt[p]{2}$ and ζ a primitive p^{th} root of unity.

$x^p - 2$ is Eisenstein at 2 $\Rightarrow$ irreducible.

The p distinct roots are $\{\alpha, \zeta\alpha, \zeta^2\alpha, \dots, \zeta^{p-1}\alpha\}$

Since $\zeta = \zeta\alpha/\alpha$, the splitting field is equivalently $\mathbb{Q}(\alpha,\zeta)$.

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\alpha,\zeta) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta) \arrow[dr, dash, "p-1"'] & & \mathbb{Q}(\alpha) \arrow[dl, dash, "p"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

- $\gcd(p, p-1) = 1 \Rightarrow [\mathbb{Q}(\alpha,\zeta):\mathbb{Q}] = p(p-1)$.
- Since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois, $\mathbb{Q}(\zeta)$ is normal.
- $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cap \mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1\}$ by coprimeness of orders.

  They generate $\mathrm{Gal}(\mathbb{Q}(\alpha,\zeta)/\mathbb{Q})$.

$\Rightarrow$ $\mathrm{Gal}(\mathbb{Q}(\alpha,\zeta)/\mathbb{Q})$ is a semidirect product

of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong C_{p-1} = \langle a \rangle$

and $\mathrm{Gal}(\mathbb{Q}(\alpha,\zeta)/\mathbb{Q}(\alpha))$ which is order $p \Rightarrow \cong C_p = \langle b \rangle$

So the elements are $\{a^i b^j \mid 0 \le i \le p-2,\ 0 \le j \le p-1\}$.

underlying set!