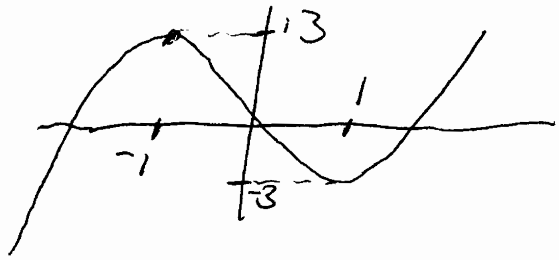
$\boxed{\text{HW \#9}}$

$\boxed{8.4\#1}$. $f'(x) = 10x^4 - 10 = 10(x-1)(x+1)(x^2+1)$ has two real roots (at $x = \pm 1$). $f(-1) = 13$, $f(1) = -3$, so f looks like



As in Thm 8.4.8, $f(x)$ has 3 real roots and hence exactly 2 complex roots. Thus complex conjugation is a transposition in the Galois group G, which is a subgroup of S_5.

Again as in Thm 8.4.8, G also contains a 5-cycle.

By Lemma 8.4.7, $G \cong S_5$.

$\boxed{8.4\#5}$ Claim: A primitive 9^{th} root of unity ~~satisfies~~ has min'l poly $x^6 + x^3 + 1$.

Then $\zeta + \zeta^8 = \zeta - \zeta^5 - \zeta^3$

$\zeta^2 + \zeta^7 = \zeta^2 - \zeta^4 - \zeta$

$\zeta^4 + \zeta^5$

are all distinct. (Otherwise ζ would satisfy a poly of degree < 6)

(2)

So it suffices to show that each of these satisfies

$x^3 - 3x + 1$.

$$(\rho+\rho^8)^3 - 3(\rho+\rho^8)+1 = \rho^{24} + 3\rho^{17} + 3\rho^{10} + \rho^3 - 3\rho - 3\rho^8 + 1$$
$$= \rho^6 + 3\rho^8 + 3\rho + \rho^3 - 3\rho - 3\rho^8 + 1$$
$$= \rho^6 + \rho^3 + 1$$
$$= 0.$$

The other two are similar.

$\boxed{8.4 \ \#6}$

$$\det\begin{pmatrix} 1 & \rho_1 & \rho_1^2 & \cdots & \rho_1^{n-1} \\ \vdots & & & & \vdots \\ 1 & \rho_n & \rho_n^2 & \cdots & \rho_n^{n-1} \end{pmatrix} \overset{\text{(Using hint)}}{=} \det\begin{pmatrix} 1 & \rho_1-\rho_n & \rho_1^2-\rho_n\rho_1 & \cdots & \rho_1^{n-1}-\rho_n\rho_1^{n-2} \\ \vdots & & & & \vdots \\ 1 & \underset{0}{\rho_n-\rho_n} & \underset{0}{\rho_n^2-\rho_n\rho_n} & \cdots & \underset{0}{\rho_n^{n-1}-\rho_n\rho_n^{n-2}} \end{pmatrix}$$

expand along bottom row

$$= (-1)^n \det\begin{pmatrix} \rho_1-\rho_n & \rho_1^2-\rho_n\rho_1 & \cdots & \rho_1^{n-1}-\rho_n\rho_1^{n-2} \\ \vdots & & & \vdots \\ \rho_{n-1}-\rho_n & \rho_{n-1}^2-\rho_n\rho_{n-1} & \cdots & \rho_{n-1}^{n-1}-\rho_n\rho_{n-1}^{n-2} \end{pmatrix}$$

(factor $\rho_i - \rho_n$ from each row)

$$= (\rho_1-\rho_n)\cdots(\rho_{n-1}-\rho_n)(-1)^n \det\begin{pmatrix} 1 & \rho_1 & \cdots & \rho_1^{n-1} \\ \vdots & & & \vdots \\ 1 & \rho_{n-1} & \cdots & \rho_{n-1}^{n-1} \end{pmatrix}.$$

$$= (\rho_n - \rho_1)\cdots(\rho_n - \rho_{n-1}) \prod_{1 \le i < j \le n-1} (\rho_j - \rho_i)$$

$\nwarrow$ by induction

$$= \prod_{1 \le i < j \le n} (\rho_j - \rho_i).$$

8.4 #7 Hint: Use Lemma 8.4.7 as a guide.

8.4 #8 $f(x)$ irred deg $p \Rightarrow G$ contains a p-cycle.

2 complex roots $\Rightarrow$ complex conjugation is a transposition in G.

By Ex 8.4 #7, $G \cong S_p$.

8.5 #1

(a) $\Phi_8(x) = x^4+1$.

(b) $\Phi_9(x) = x^6+x^3+1$.

(c) $\Phi_{15}(x) = x^8-x^7+x^5-x^4+x^3-x+1$.

(d) $\Phi_{20}(x) = x^6-x^5+x-1$.

$\boxed{8.5 \# 2}$ Note $x^{2^k}-1=(x^{2^{k-1}}-1)(x^{2^{k-1}}+1)$, and every primitive 2^k th root is a root of $(x^{2^{k-1}}+1)$. $\Rightarrow \Phi_{2^k}(x) \mid (x^{2^{k-1}}+1)$

Since $\deg \Phi_{2^k}(x) = \varphi(2^k) = 2^{k-1}$, we have equality.

$\boxed{8.5 \# 3}$ If ζ is a primitive p^k th root of 1, then $\zeta^{p^{k-1}}$ is a primitive p^{th} root of 1.

$\Rightarrow \Phi_{p^k}(x) \mid \Phi_p(x^{p^{k-1}})$.

Since $\deg \Phi_{p^k}(x) = \varphi(p^k) = p^{k-1}\underbrace{(p-1)}_{\deg \Phi_p}$,

we're done.

$\boxed{8.5 \# 7}$ We need to check that all the field axioms hold for D.

- Clearly $0, 1 \in D$ and $x \in D \Rightarrow -x \in D$.
- $x, y \in D$. Need $x+y \in D$. This is equivalent to $(x+y)d = d(x+y)$ $\forall d \in D$.

  But $(x+y)d = xd+yd \underset{x,y \in D}{=} dx+dy = d(x+y)$ ✓

5

• Similarly check $x, y \in D \Rightarrow xy \in D$ and $x^{-1} \in D$.

$\boxed{8.5 \# 9}$ Recall $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

So $\prod_{n|m} (x^n - 1)^{\mu(m/n)} = \prod_{n|m} \prod_{d|n} \Phi_d(x)^{\mu(m/n)}$.

What's the exponent on $\Phi_d(x)$? It's

$$\sum_{\substack{n \text{ s.t.} \\ d|n,\ n|m}} \mu(m/n) = \sum_{n'|m'} \mu\left(\frac{m'}{n'}\right) = \sum_{n'|m'} \mu(n')$$

divide everything by d.

$\frac{m}{n} = \frac{m'}{n'}$

$\left\{\frac{m'}{n'}\right\}$ consists of all divisors of m'.

Prop 6.6.6 says $\sum_{n'|m'} \mu(n') = \begin{cases} 1 & \text{if } m' = 1 \\ 0 & \text{if } m' > 1 \end{cases}$

Since $m' = \frac{m}{d}$, this says that the exponent on

$\Phi_d(x)$ is $\begin{cases} 1 & \text{if } d = m \\ 0 & \text{otherwise.} \end{cases}$

This finishes the problem.

6

$\boxed{8.5 \ \#10}$

a) ζ prim. mp^k th root of $1 \Rightarrow \zeta^{p^{k-1}}$ is a prim mp th root of 1. $\deg(\Phi_{mp^k}) = \varphi(mp^k) = \varphi(m)\varphi(p^k)$ ← $\gcd(m,p)=1$

$= \varphi(m)(p-1)p^{k-1}$

$= \varphi(m)\varphi(p)p^{k-1}$

$= \varphi(mp)p^{k-1}$ //

b) $\underbrace{\Phi_{pm}(t)}_{\deg \varphi(pm) = (p-1)\varphi(m)} \ \underbrace{\Phi_m(t)}_{\deg \varphi(m)} \stackrel{?}{=} \underbrace{\Phi_m(t^p)}_{\text{degree } p\cdot\varphi(m)}$

So the degrees are the same.

- ζ a prim pm th root of 1, $\Rightarrow \zeta^p$ is a prim m th root of 1.
- Let ζ be a prim m th root of 1. As $\gcd(p,m)=1$, ζ^p is still a prim. m th root of 1.

Thus LHS | RHS.

c) The only difference between this and #9 is the presence of a factor of

$$(-1)^{\sum_{d|n}\mu(d)} = (-1)^0 = 1 \text{ if } n>1.$$

(d) Let ζ be a prim $2n^{th}$ root of 1.

$\Rightarrow \zeta^{2n} = 1 \Rightarrow \zeta^n = -1.$

But then $(-\zeta)^n = (-1)^n \zeta^n = (-1)^{n+1} = 1$, so

$-\zeta$ is a prim. n^{th} root of 1.

$\Rightarrow \Phi_{2n}(t) \mid \Phi_n(-t).$

But $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$, so we have equality.

$\boxed{8.6 \# 1}$ If $f(x) = x^n + \frac{b_{n-1}}{d} x^{n-1} + \cdots + \frac{b_1}{d} x + \frac{b_0}{d}$,

then $d^n f\left(\frac{x}{d}\right) = d^n\left[\frac{x^n}{d^n} + \frac{b_{n-1}}{d}\left(\frac{x^{n-1}}{d^{n-1}}\right) + \cdots + \frac{b_1}{d}\left(\frac{x}{d}\right) + \frac{b_0}{d}\right]$

$$= x^n + b_{n-1} x^{n-1} + \cdots + b_1 d^{n-2} x + b_0 d^{n-1}$$

$$\in \mathbb{Z}[x].$$

If α is a root of $f(x)$, then $d\alpha$ is a root of $d^n f\left(\frac{x}{d}\right)$. So $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(d\alpha_1, \ldots, d\alpha_n)$.

$\boxed{8.6\#2}$ Automatically $G \leq S_3$ and contains a 3-cycle $\Rightarrow$ $G = \mathbb{Z}_3$ or $G = S_3$.

Prop 8.6.6 say Δ is a square $\Leftrightarrow$ every elt of G is even. So

$$\begin{cases} \Delta \text{ a square} \Rightarrow G = \mathbb{Z}_3 \ (\cong A_3) \\ \Delta \text{ not a sq.} \Rightarrow G = S_3. \end{cases}$$

$\boxed{8.6\#3}$ $\mathbb{Z}_3$: $x^5 - x - 1$ is irreducible.

$\mathbb{Z}_2$: $x^5 - x - 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$

By Theorem (Dedekind, p 402) G contains (5 cycle) and (2 cycle)(3 cycle).

But note $((a\,b)(c\,d\,e))^3 = (a\,b) \in G$.

By Lemma 8.4.7, $G \cong S_5$.

$\boxed{8.6\#4}$

$\mathbb{Z}_2$: Irreducible $\Rightarrow G \leq S_4$ contains a 4-cycle.

$\mathbb{Z}_3$: $x^4 + 2x^2 + x + 3 = x(x^3 - x + 1) \Rightarrow G$ contains a 3-cycle.

By Wolfram Alpha, the discriminant is 3877, which is not a square. Prop 8.6.6 $\Rightarrow$ not every elt of G is even.

By 8.6 #5, the transitive subgroups of S_4 are

S_4

$\cancel{A_4}$ not all elts even

$\cancel{D_4}$ no 3-cycle

$\cancel{\mathbb{Z}_4}$ no 3-cycle

$\cancel{\mathbb{Z}_2 \times \mathbb{Z}_2}$ no 3-cycle or 4-cycle.

$\Rightarrow G \cong S_4$.

$\boxed{8.6 \# 5}$ find yourself a list of subgroups of S_4 (like Ex 7.4 # 8) and check explicitly.

$\boxed{8.6 \# 12}$

Calculation. &