HW 6

(1) a) $G_{K/\mathbb{Q}}$ acts transitively on the roots $\alpha_1 \dots \alpha_n$ of f as f is irreducible.

let p ur in K $\quad \mathrm{Frob}_{\mathfrak{P}/p} \in G_{k_{\mathfrak{P}}/\mathbb{F}_p}$

$\uparrow\uparrow$

$G_{K/\mathbb{Q}}$

and $\langle \mathrm{Frob}_{\mathfrak{P}/p} \rangle$ acts transitively on the roots of

$\| \; G_{k_{\mathfrak{P}}/\mathbb{F}_p}$

the irreducible factor of $f \bmod \mathfrak{P}$ corresponding to $\mathfrak{P}$.

But f splits completely modulo p for almost all p.

For such a p, $\mathrm{Frob}_{\mathfrak{P}/p} = 1 \quad \forall\, \mathfrak{P} \mid p$.

By Chebotarev $\delta(p \mid \mathrm{Frob}_p = 1) = \frac{1}{|G_{K/\mathbb{Q}}|}$

and we just showed $\delta(p \mid \mathrm{Frob}_p = 1)$

$= \delta(p \mid p \gg 0) = 1 \qquad$ so $K = \mathbb{Q}$

so $\deg f = 1$.

b). Each irreducible factor of f satisfies (a) so must be linear

(2) (a) optional ——

(b) (i) Let K = splitting field over $\mathbb{Q}$ and $G = Gal(K/\mathbb{Q})$

$X = \{\alpha_1, \dots \alpha_n\}$ = roots of $f(x)$.

Then G acts faithfully and transitively on X if irreducible

(an automorphism is defined by what it does on the roots)

so by (a) if $\deg f > 1$ $\exists\, \sigma \in G$ s.t.

$\sigma(\alpha) \neq \alpha$ for $f(\alpha) = 0$.

(ii) Follows from Chebotarev.

(iii) Suppose $p >> 0$ s.t. $f(x) \bmod p$ has a linear factor and let $\mathfrak{P}$ = prime ideal of this factor of $\mathbb{Q}(\alpha)$.

Let α be a root of f. $\rightsquigarrow$

Then as in Problem 1, $Frob_{\mathfrak{P}/p}$ acts transitively on the single root $\overline{\alpha_{\mathfrak{P}}}$ of this irreducible polynomial mod p and so $Frob_{\mathfrak{P}/p} = 1$

This implies that if $q \mid \mathfrak{P}$ in K

Then $Frob_{q/p}$ fixes $\overline{\alpha_{\mathfrak{P}}} \in \mathbb{F}_p$.

The roots $\alpha_1, \dots \alpha_n$ are distinct and so $\alpha_i - \alpha_j \neq 0$ for $i \neq j$ so $\forall$ prime p is coprime to all $\alpha_i - \alpha_j$.

$p >> 0$

Now pick p st $\text{Frob}_p = \{g\sigma g^{-1}\}$

and $\text{Frob}_{q/p} = \sigma$ in it.

Then $\sigma = \text{Frob}_{q/p}$ doesn't fix α_i so

$$\sigma(\alpha_i) = \alpha_j \quad \text{for } j \neq i$$

and so $\sigma(\alpha_i) \not\equiv \alpha_i \pmod{p}$. $\forall\, i$

But $\text{Frob}_{q/p}(\bar{\alpha}_{\mathfrak{P}}) \equiv \bar{\alpha}_{\mathfrak{P}} \pmod{p}$

and $\bar{\alpha}_{\mathfrak{P}}$ = reduction mod $\mathfrak{P}$ of some α_i

We get a contradiction so $\deg f = 1$.

(3) (a) $x^2 - a$ has a root in $\mathbb{F}_p$

$\Leftrightarrow$ a is a perfect square. But $\mathbb{F}_p^\times = \{g\}$

$\cong \mathbb{Z}/(p-1)\mathbb{Z}$

is cyclic so this occurs

$\Leftrightarrow a = g^\alpha$ α odd.

If $x^2 - 2$ and $x^2 - 3$ don't have a root then $2 = g^{2\alpha+1}$ $3 = g^{2\beta+1}$

so $6 = g^{2\alpha+2\beta+2}$ is a perfect square

so $x^2 - 6$ has a root.

(b) if $p \equiv 1 \pmod 3$ then we already know $x^2 + x + 1 \equiv 0 \pmod p$ has a root from a previous homework.

Suppose $p \equiv 2 \pmod 3$. Then

$X = 2^{-\frac{p-2}{3}} \pmod p$ satisfies

$$X^3 \equiv 2^{-(p-2)} \pmod p \equiv 2^{-(p-1)+1} \equiv 2 \pmod p$$

Finally if $p = 2$ then 0 is a root mod p.

(c) By 2(b) f cannot be irreducible and the requirement that f have no roots in $\mathbb{Z}$ implies that all irreducible factors of f have degree ≥ 2.

Thus $\deg f \geq 2 \times 2 = 4$. We need only to rule out the case $f(x) = (x^2 - a)(x^2 - b)$ for $a, b \in \mathbb{Z}$, a, b square free $\neq 1$. Let $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ Galois over $\mathbb{Q}$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^2$ as $\mathbb{Q}(\sqrt{a}) \cap \mathbb{Q}(\sqrt{b}) = \mathbb{Q}$.

The roots are $\pm\sqrt{a}$, $\pm\sqrt{b}$ so $G_{K/\mathbb{Q}} \subset S_4$
$\quad 1,2 \quad 3,4$

Consists of $\{1; (12), (34), (12)(34)\}$.

By Chebotarëv $\exists$ infinitely many p s.t. $\mathrm{Frob}_p = (12)(34)$

The image of Frob_p in $G_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}$ is (12), $\sqrt{a} \mapsto -\sqrt{a}$

in $G_{\mathbb{Q}(\sqrt{b})/\mathbb{Q}}$ is $(3,4)$, $\sqrt{b} \mapsto -\sqrt{b}$

and so Frob_p of $\mathbb{Q}(\sqrt{a}) \neq 1$

Frob_p of $\mathbb{Q}(\sqrt{b}) \neq 1$

but x^2-a or x^2-b has root mod p would imply Frob$_p$ of $\mathbb{Q}(\sqrt{a})$ or Frob$_p$ of $\mathbb{Q}(\sqrt{b})$ is trivial

(4) (a) $\frac{1}{n} = 0.\underbrace{a_1 \cdots a_k}_{A}\,\underbrace{(b_1 \cdots b_\ell)}_{B}$ in base 10

$\Rightarrow$

$$\frac{10^k}{n} = A + \underbrace{0.(b_1 \cdots b_\ell)}_{y}$$

$$y \cdot 10^\ell = B + 0.(b_1 \cdots b_\ell) = B + y$$

so $$y = \frac{B}{10^\ell - 1}$$

$$\frac{10^k}{n} = A + \frac{B}{10^\ell - 1}$$

n coprime to 10 means that we may take $k=0$, $A=0$

$$\frac{1}{n} = \frac{B}{10^\ell - 1} \Rightarrow n \mid 10^\ell - 1$$

and reciprocally $n \mid 10^\ell - 1 \Rightarrow \frac{1}{n} = \frac{\left(\frac{10^\ell - 1}{n}\right) = B}{n}$

So ℓ = length of period
= order of 10 mod n.

(b) From homework 3 p splits completely in $\mathbb{Q}(\zeta_{2^k})$ iff $2^k \equiv 1 \pmod p$ iff Φ_{2^k} splits completely mod p.

(c) First $\ell = 2^k$ in $\mathbb{Q}(\zeta_{2^{k+1}})$ no does not split in $\mathbb{Q}(\zeta_{2^k})$ $\Rightarrow$ p does not split in $\mathbb{Q}(\zeta_{2^{k+1}})$.

(c) $\sqrt[n]{a}$ can go to $\zeta_n^k \sqrt[n]{a} \in \mathbb{Q}(\sqrt[n]{a}, \zeta_{nd})$

ζ_{nd} can go to ζ_{nd}^{ℓ}

$\sigma_{k,\ell}(\sqrt[n]{a}) = \zeta_n^k \sqrt[n]{a}$ $\quad 0 \le k \le n-1$

$\sigma_{k,\ell}(\zeta_{nd}) = \zeta_{nd}^{\ell}$ $\quad \ell \in (\mathbb{Z}/nd\mathbb{Z})^*$

so $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{a}, \zeta_{nd})) \cong (\mathbb{Z}/nd\mathbb{Z})^* \rtimes (\mathbb{Z}/n\mathbb{Z})$

in fact $\cong \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \begin{array}{l} x \in (\mathbb{Z}/nd\mathbb{Z})^* \\ y \in \mathbb{Z}/n\mathbb{Z} \end{array} \right\}$

where $x \cdot y$ is defined by first projecting x to $(\mathbb{Z}/n\mathbb{Z})^*$.

(d) First if $p-1 = 2^k m$ m odd

$\Rightarrow$ p does not split in $\mathbb{Q}(\zeta_{2^{k+1}})$ so does not split in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})$.

$L = \mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})$ $\quad$) 2^k

$K = \mathbb{Q}(\zeta_{2^k})$ $\quad$) $\varphi(2^k)$

$\mathbb{Q}$

by (c) $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2^k\mathbb{Z}$

so $X^{2^k} - 10$ is min poly of $\sqrt[2^k]{10}$ over $\mathbb{Q}(\zeta_{2^k})$.

and $L = K(\sqrt[2^k]{10})$.

L/K is Galois so it suffices to show that if

$p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ where $f_{\mathfrak{p}_i/p} = 1$ (splits completely)

$e_{\mathfrak{p}_i/p} = 1$

$r = \varphi(2^k)$

then each $\mathfrak{p}_i$ splits completely in L.

From pset 3 the splitting of $\mathfrak{p}_i$ in L is governed by the splitting of $X^{2^k} - 10 = \text{min poly } \sqrt[2^k]{10}$ over K modulo $\mathfrak{p}_i$

but $k_{\mathfrak{p}_i} = \mathbb{F}_p$ $(f_{\mathfrak{p}_i/p} = 1)$

so we need splitting of $x^{2^k} - 10$ in $\mathbb{F}_p[x]$.

It has one root in $\mathbb{F}_p$ so some $q \mid \mathfrak{p}_i$ st

$f_{q_i/\mathfrak{p}_i} = e_{q_i/\mathfrak{p}_i} = 1$. By L/k Galois

$\Rightarrow$ $\mathfrak{p}_i$ splits completely in L.

(e) p splits completely in $L = \mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})$

$\Rightarrow$ it splits in $K = \mathbb{Q}(\zeta_{2^k})$ $\rightarrow$ $2^k \mid p-1$.

Moreover, $X^{2^k} - 10$ must split in $k_{\mathfrak{p}}[x] = \mathbb{F}_p[x]$

$\forall \mathfrak{p} \mid p$ prime of $\mathbb{Q}(\zeta_{2^k})$.

if $2^{k+1} \mid p-1$ then p splits completely

in $\mathbb{Q}(\zeta_{2^{k+1}})$ so must split in the composite

$\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})\,\mathbb{Q}(\zeta_{2^{k+1}}) = \mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})$ $\square$.

(f) $\ell(p)$ = smallest integer r such that $10^r \equiv 1 \pmod p$

Write $p-1 = 2^k m$. Then $r \mid p-1$

and r is odd $\iff$ $r \mid m$ $\iff$ $r \mid \frac{p-1}{2^k}$.

$\iff$ $10^{\frac{p-1}{2^k}} \equiv 1 \pmod p$

Write g for a generator of $\mathbb{F}_p^\times$. Then $10^{\frac{p-1}{2^k}} \equiv 1 \iff$

$10 = g^{2^k \cdot \alpha}$ for some $\alpha \in \mathbb{Z}$

so $(g^\alpha)^{2^k} \equiv 10 \pmod p$ so $X^{2^k} \equiv 10 \pmod p$

has a root $g^\alpha \in \mathbb{F}_p$.

By the above this is equivalent to p splitting completely in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})$ but not in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})$.

(h). If p splits completely in $L_k = \mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})$ then it does not in $K_k = \mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})$

so $\{ p \mid p$ splits completely in K_k but not in $L_k \} =$

$= \{ p \mid p$ splits completely in $K_k \} \setminus$

$\setminus \{ p \mid p$ splits completely in $L_k \}$.

so $\delta(\{ p$ splits in K_k but not in $L_k \})$

$= \delta(\{ p$ splits in $K_k \}) - \delta(\{ p$ splits in $L_k \})$

$=$ Chebotarev $= \frac{1}{[K_k : \mathbb{Q}]} - \frac{1}{[L_k : \mathbb{Q}]} = \frac{1}{2^k \varphi(2^k)} - \frac{1}{2^{k+1}\varphi(2^k)}$

$= \frac{1}{2^{k+1}\varphi(2^k)} = \frac{1}{2^{2k}}$

splitting completely means Frob $p = 1$

$$\delta\{ \ell(p \mid \text{odd}) \} = \sum_{k \geq 1} \delta\{ p \text{ splits completely in } K_k \text{ but not in } L_k \}$$

$$= \sum_{k \geq 1} \frac{1}{2^{2k}} = \frac{1}{4} \frac{1}{1 - \frac{1}{4}} = \frac{1}{3}.$$

(5) (a) $f \bmod \mathfrak{p}$ separable $\Rightarrow$ $\mathfrak{p}$ is unramified in L

so $D_{\mathfrak{q}/\mathfrak{p}} \cong \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$ acting on the roots $\alpha_1 \cdots \alpha_n$ and $\alpha_i \bmod \mathfrak{q}$. Indeed

say $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$ $\quad \sigma(\alpha_i) \bmod \mathfrak{q} = \sigma(\alpha_i) \bmod \sigma(\mathfrak{q}) = \sigma(\alpha_i \bmod \mathfrak{q})$

$\mathfrak{q} = \sigma(\mathfrak{q})$ as $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$

(b) Let $f(X) \equiv f_1(X) \cdots f_r(X) \pmod{\mathfrak{p}}$

in which case $\mathfrak{p} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ (from Pset 3)

$f_{\mathfrak{q}_i/\mathfrak{p}} = \deg f_i(X)$

and so $\mathrm{Frob}_{\mathfrak{q}_i/\mathfrak{p}}$ permutes the roots of $f_i(X)$ as it generates $\mathrm{Gal}(k_{\mathfrak{q}_i}/k_{\mathfrak{p}})$ cyclic of order $f_{\mathfrak{q}_i/\mathfrak{p}}$.

Thus $\mathrm{Frob}_{\mathfrak{p}}$ permutes cyclically each set of roots of $f_i(X)$ and so as a permutation it is

$\mathrm{Frob}_{\mathfrak{p}} = c_1 \cdots c_r$ where c_i = cycle length $\deg f_i(X)$.

(c) $f(X) = X^5 - X + 1$

(i) Suppose α is a root of $f(X) \bmod 5$. Then

$$f(\alpha + i) = (\alpha+i)^5 - (\alpha+i) + 1$$
$$\equiv \alpha^5 + i^5 - \alpha - i + 1$$
$$\equiv \alpha^5 - \alpha + 1 \equiv 0 \pmod 5$$

for $i = 0, 1, 2, 3, 4$

Thus either $f(X)$ is irreducible mod 5 or it splits into linear factors. Indeed, $\sigma(\alpha) = \alpha+1$ gives an element of Gal(splitting field of f mod $5/\mathbb{F}_5$) and $\sigma^5 = 1$.

But $f(X)$ has no roots mod 5 so must be irreducible mod 5 $\Rightarrow$ it is irreducible in $\mathbb{Z}[X]$.

(ii) f mod 5 is irreducible so by (b)

$\Rightarrow$ Frob 5 = 5-cycle.

$$f(X) \bmod 2 \equiv X^5 + X + 1$$
$$\equiv X^5 + 2X^4 + 2X^3 + 2X^2 + X + 1$$
$$\equiv X^5 + X^4 + X^3 + X^4 + X^3 + X^2 + X^2 + X + 1$$
$$\equiv (X^2 + X + 1)(X^3 + X^2 + 1)$$

each is irreducible mod 2 as they have no roots. By (b) Frob 2 = $\tau \cdot \nu$

τ = transposition

ν = 3-cycle

$\Rightarrow$ $\text{Frob}_2^3 = \tau^3 = \tau$ = 2-cycle

Thus Gal$(K/\mathbb{Q})$ contains a 2-cycle & 5-cycle

$\rightarrow \cong S_5$

(iii') $f \bmod P = f_{i_1} \cdots f_{i_k} \pmod 5$ $\quad n_1 \cdots n_k$

$\overset{(b)}{\Longleftrightarrow}$ $\quad \mathrm{Frob}_p = n_1\text{-cycle} \times \cdots \times n_k\text{-cycle}$

and in S_n the conjugacy class of n_1-cycle $\times \cdots \times n_k$-cycle

$= \{$ set of all n_1-cycle $\times \cdots \times n_k$-cycle $\}$

Tells by Chebotarëv

$\delta\{p \mid f \bmod p = f_{i_1} \cdots f_{i_k}$ of degs $n_1 \cdots n_k\}$

$= \delta\{p \mid \mathrm{Frob}_p = \{n_1\text{-cycle} \times \cdots \times n_k\text{-cycle}\}\}$

$= \dfrac{n_{i_1} \cdots i_k}{|S_5|} = \dfrac{n_{i_1} \cdots i_k}{120}$.

(iv) Need to count 2-cycles × 3-cycles and 5-cycles

2-cycles × 3-cycles : $(ab)(cde)$ $\quad a<b$ $\quad c<d<e$

and $(a<b)\ (ced)$ $\quad c<d<e$

so total # is $\binom{5}{2} \times 2 = 20$

so density is $\dfrac{20}{120} = \dfrac{1}{6}$.

5-cycles shift so that 5-cycle looks like $(1\ a\ b\ c\ d)$ $\quad a,b,c,d$ any choice

in which case total # is $4! = 24$

so density $= \dfrac{24}{120} = \dfrac{1}{5}$