Algebraic Number theory

Ex Sheet 2 Rough solutions

1. $A = \mathbb{Z}_{(5)}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$

$B = \mathbb{Z}[i]_{(5)}$ (localisation at $5\mathbb{Z}[i]$).

this has two primes (up to units):

$2-i$ and $2+i$.

2. We have

$$f_{M|K} = [k_M : k_K] = [k_M : k_L][k_L : k_K] =$$

$$= f_{M|L} f_{L|K}.$$

then

$$e_{M|K} = \frac{[M:K]}{f_{M|K}} = \frac{[M:L]}{f_{M|L}} \frac{[L:K]}{f_{L|K}} =$$

$$= e_{M|L} e_{L|K}.$$

3 (i) Consider the Teichmüller lift

$$[\cdot] : k_K \longrightarrow \mathcal{O}_K \subseteq K .$$

Then $[x]^q = [x^q] = [x] \quad \forall x \in k_K$,

so K contains the splitting field of $X^q - X$,

which is $\mathbb{F}_q$.

So in fact $[-]$ is additive, hence

a homomorphism.

Now let $\pi_K \in \mathcal{O}_K$ be a uniformizer.

Then any element $x \in \mathcal{O}_K$ can be written

uniquely as

$$x = \sum [y_n] \pi_K^n , \quad y_n \in k_K ,$$

so choosing an isomorphism $k_K \overset{\phi}{\cong} \mathbb{F}_q$ we get

an isomorphism

$$\begin{aligned} \mathcal{O}_K &\xrightarrow{\sim} \mathbb{F}_q[[t]] \\ [y] &\longmapsto \phi(y) \\ \pi_K &\longmapsto t . \end{aligned}$$

Thus ~~...~~ implies $K \cong \mathbb{F}_q((t))$.

(ii) Consider $\mathbb{Q} \leq K$, and let v be the valuation on K, normalised so that $v(p) = 1$.

Then $v|_{\mathbb{Q}} = v_p$ by Q13, Sheet 1.

If $|x| = p^{-v(x)}$, then $|\cdot|\,|_{\mathbb{Q}} = |\cdot|_p$, and K complete $\Rightarrow$ $K \supseteq \mathbb{Q}_p$ since $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ wrt $|\cdot|_p$.

Let $\bar{x} \in k_K$ be a primitive element of $k_K | \mathbb{F}_p$. Set $f = [k_K : \mathbb{F}_p]$ and define e by $v(\pi_K) = \frac{1}{e}$, where $\pi_K \in \mathcal{O}_K$ is a uniformizer.

~~...~~ Set $x = [\bar{x}] \in \mathcal{O}_K$, then $x^q = x$, so x is integral ~~of~~ over $\mathbb{Z}_p$.

Moreover, $\mathbb{Z}_p[x] \leq \mathcal{O}_K$ contains all Teichmüller lifts and is finite over $\mathbb{Z}_p$.

Set $M = \bigoplus_{i=0}^{e-1} \mathbb{Z}_p[x]\pi_K^i \subseteq \mathcal{O}_K$;

this is a f.g $\mathbb{Z}_p$-submodule of $\mathcal{O}_K$ (but not nece a ring, a priori).

Claim $M = \mathcal{O}_K$.

To see this, note that $M + \pi_K^e \mathcal{O}_K = \mathcal{O}_K$ by looking at expansions

$$x = \sum_{i \geq 0} [y_n] \pi_K^i \quad , \; y_n \in k_K.$$

Now $\pi_K^e \mathcal{O}_K = p\mathcal{O}_K$, so $\mathcal{O}_K = M + p\mathcal{O}_K$.

We get $\mathcal{O}_K = M + p\mathcal{O}_K = M + p(M + p\mathcal{O}_K) =$

$$= M + p^2\mathcal{O}_K = M + p^2(M + p\mathcal{O}_K) =$$

$$= M + p^3\mathcal{O}_K = \ldots ,$$

so $M + p^n\mathcal{O}_K = \mathcal{O}_K \ \forall n \Rightarrow$

M is dense in $\mathcal{O}_K$. But M is closed by the hint, so $M = \mathcal{O}_K$.

It follows that $\mathcal{O}_K$ is finite over $\mathbb{Z}_p$, and hence that K is a finite ext^n of $\mathbb{Q}_p$.

4. (i) <u>Newton–Raphson</u>

Set $x_1 = x$, $x_{n+1} = x_n - \dfrac{f(x_n)}{f'(x_n)}$

for $n \geq 1$. Let $t = v(f(x)) - 2v(f'(x)) > 0$.

<u>Claim</u>: 1) x_n is well-defined, and in A.

2) $v(f'(x_n)) = v(f'(x))$ $\forall n$.

3) $v(f(x_n)) \geq 2v(f'(x_n)) + 2^{n-1}t$

We prove this by induction on n; the case $n = 1$ follows from assumptions.

Assume it holds for n.

1) $$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} \in A \quad \text{by 1)+3) for } n.$$

2) $$f'(x_{n+1}) - f'(x_n) = (x_{n+1} - x_n)\, y$$

for some $y \in A$, so

$$v(f'(x_{n+1}) - f'(x_n)) \geqslant v(x_{n+1} - x_n) =$$

$$= v(f(x_n)) - v(f'(x_n)) \geqslant v(f'(x_n)) + 2^{n-1} t$$

$$> v(f'(x_n))$$

using 3) for n, so

$$v(f'(x_{n+1})) = v(f'(x_n)) = v(f'(x_1)) \text{ by}$$

2) for n.

3) $$f(x_{n+1}) = f(x_n) + (x_{n+1} - x_n) f'(x_n) +$$

$$+ z(x_{n+1} - x_n)^2 \quad \left(\begin{array}{c}\text{for some} \\ z \in A\end{array}\right)$$

$$= \frac{f(x_n)^2}{f'(x_n)^2} z, \quad \text{so}$$

$$v(f(x_{n+1})) \geq 2\left(v(f(x_n)) - v(f'(x_n))\right) \geq$$
$$\geq 2\left(v(f'(x_n)) + 2^{n-1}t\right) =$$
$$= 2v(f'(x_{n+1})) + 2^n t$$

using 3) for n and 2) for $n+1$.

This finishes the induction, shows that

$$\alpha = \lim_{n\to\infty} x_n \text{ exists and satisfies } f(\alpha) = 0$$

and $v(\alpha - x) > v(f'(x))$

Uniqueness: Suppose β is another root with the same properties. Write $\beta = \alpha + h$, assume $h \neq 0$, get

$$0 = f(\beta) = f(\alpha) + (\beta-\alpha)f'(\alpha) + (\beta-\alpha)^2 w$$
$$(\text{some } w \in A) \quad = h f'(\alpha) + h^2 w$$

$$\Rightarrow \quad f'(\alpha) = -hw \quad \Rightarrow \quad v(f'(\alpha)) \geq v(h).$$

But $v(h) = v(\beta - \alpha) \geq \min\left(v(\alpha - x), v(\beta - x)\right) >$
$$> v(f'(x)) = v(f'(\alpha)) \quad \#$$

(ii) Choose monic lifts $g_0, h_0 \in A[T]$ of $\bar{g}, \bar{h}$. Choose $a, b \in A[T]$ s.t

$$a g_0 + b h_0 \equiv 1 \mod \pi.$$

Want to construct, by induction on n, polynomials $p_1, \ldots$ & $q_1, \ldots$ s.t

1) If $g_n = g_0 + \pi p_1 + \pi^2 p_2 + \ldots + \pi^n p_n$

$$h_n = h_0 + \pi q_1 + \ldots + \pi^n q_n,$$

then $f - g_n h_n \equiv 0 \mod \pi^{n+1}$

2) ~~q_n & p_n have bounded~~ ~~max{deg~~

deg p_n < deg g_0, deg q_n < deg h_0.

$n = 0$ is clear.

$\underline{\underline{n \geq 1}}$: Set $f_n = \pi^{-n}(f - g_{n-1}h_{n-1}) \in A[T]$.

For any p_n, q_n, we have

$$f - (g_{n-1} + \pi^n p_n)(h_{n-1} + \pi^n q_n) \equiv$$

$$\equiv f - g_{n-1}h_{n-1} + \pi^n(g_{n-1}q_n + h_{n-1}p_n) \equiv$$

$$\equiv \pi^n\left(-f_n + g_{n-1} q_n + h_{n-1} p_n\right) \mod \pi^{n+1}$$

$\Rightarrow$ ~~So~~ we want p_n, q_n s.t.

$$f_n - g_{n-1} q_n + h_{n-1} p_n \equiv 0 \mod \pi$$

Have

$$f_n - g_{n-1} q_n + h_{n-1} p_n \equiv f_n - g_0 q_n + h_0 p_n \mod \pi$$

~~Set~~ Have $f_n \equiv f_n(a g_0 + h_0 b) \equiv$

$$\equiv (a f_n) g_0 + (b f_n) h_0$$

Can't set $q_n = a f_n$, $p_n = b f_n$ since the degrees might be too big.

Instead, use the division algorithm:

Define p_n by $b f_n = Q g_0 + p_n$, $\deg p_n < \deg g_0$

($p_n \in A[T]$ since g_0 monic)

Then $(af_n)g_0 + (bf_n)h_0 =$

$$= (af_n + Qh_0)g_0 + P_n h_0 \equiv f_n \mod \pi$$

Now define q_n to be the polynomial obtained from $af_n + Qh_0$ by deleting all coefficients divisible by π.

Using $\deg q_n = \deg(q_n \mod \pi)$, one checks that $\deg q_n < \deg h_0$.

This completes the induction.

~~Now~~

Now set $g = \lim_{n\to\infty} g_n$, $h = \lim_{n\to\infty} h_n$.

5. $L|K$ is Galois.

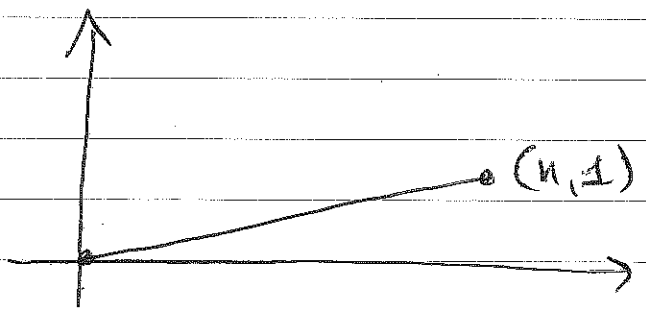
Let $\sigma \in Gal(L|K)$.

Then, $\forall i$, $v(\sigma \alpha_i) = v(\alpha_i)$ $\Longrightarrow$

$\Rightarrow$ $f_r \in L[T]$ is stable under the action of $Gal(L|K)$, so $f_r \in K[T]$.

The last assertion follows from the correspondence between the slopes of the Newton polygon & the valuations of the roots (proved in lectures).

6. i) Reformulation was done in lectures; the Newton polygon is



Let α be a root of f, then α has valuation $1/n$

Consider $L = K(\alpha)$ with w the ext^n to L of v_K; $w(\alpha) = 1/n$.

If π_L is a uniformizer of L, then

$e_{L|K}^{-1} = w(\pi_L) \leq w(\alpha) \Rightarrow$

$\Rightarrow \quad e_{L|K} \geq n$

But $e_{L|K} \leq [L:K] \leq n \quad \Rightarrow$

$\Rightarrow \quad n = [L:K]$.

But $[L:K] = \deg g$, where g is the irreducible factor of f in $K[T]$ s.t $g(\alpha) = 0$.

$\therefore f = g$, so f irreducible.

(ii) It suffices to show that

$$f_n(T) = \Phi_{p^n}(T+1) \text{ is Eisenstein.}$$

$f_n(0) = \Phi_{p^n}(1) = p$, so it suffices to show that $f_n(T) \equiv T^{p^{n-1}(p-1)}$ mod p.

We have

$$f_n(T) = (T+1)^{p^n(p-1)} + \ldots + (T+1)^{p^{n-1}} + 1 \equiv$$

$$\equiv (T^{p^{n-1}}+1)^{p-1} + \ldots + (T^{p^{n-1}}+1) + 1 \equiv$$

$$\equiv f_1(T^{p^{n-1}}) \bmod p$$

so it suffices to prove this for $n=1$.

But $f_1(T) = \dfrac{(T+1)^p - 1}{T} = \sum_{k=1}^{p} \binom{p}{k} T^{k-1} \equiv$

$$\equiv T^{p-1} \bmod p.$$

iii) The criterion is that ~~B~~ the Newton polygon of f has a single slope k/n, where k is coprime to n.

In this case, let $a, b \in \mathbb{Z}$ s.t $ak + bn = 1$. If α is a root of f and w is the ext^n of v_K to $L = K(\alpha)$, then

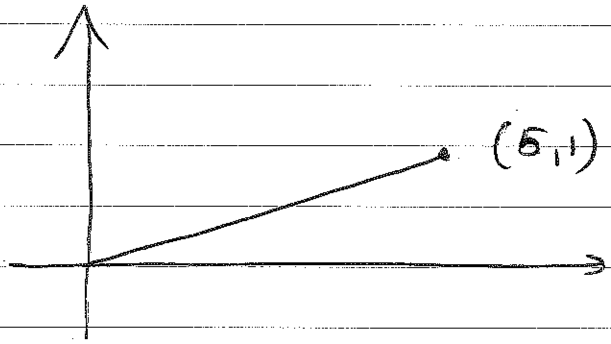
$$w\left(\alpha^a \pi_K^b\right) = \frac{ak}{n} + b = \frac{1}{n}.$$

The same proof as in 6(i) then shows that f is irreducible and $L|K$ is totally ramified.

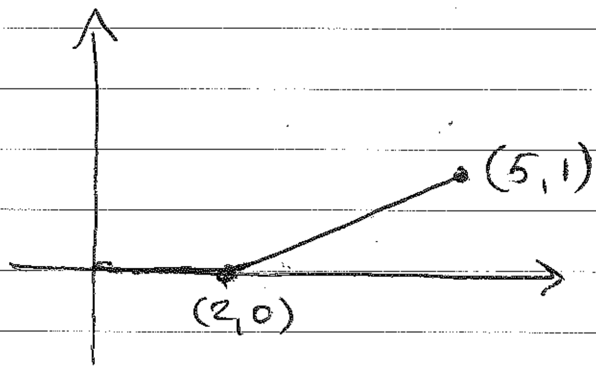
If the Newton polygon of f doesn't look like this, then either $\exists$ multiple slopes $\Rightarrow$ f reducible by Q5, or $\exists$ single slope , $v_K(a_0)/n$ and $\exists$ minimal $m | n$ s.t $m \in \{1, \dots, n-1\}$ and $k = \frac{v_K(a_0)m}{n} \in \mathbb{Z}$.

The polynomial $\left(x^m - \pi_K^k\right)^{n/m}$ is reducible and has thus Newton polygon.

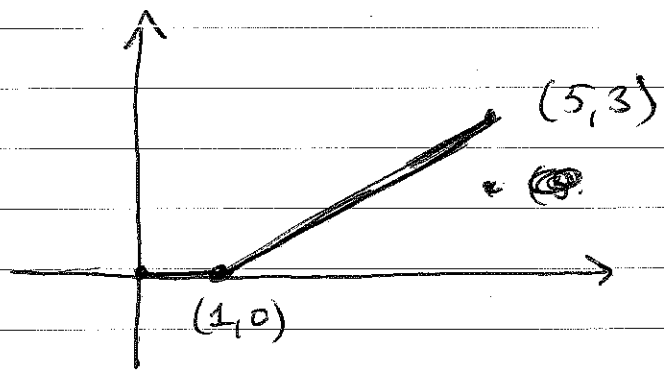
7. (i) <u>$p = 5$</u> :



<u>$p = 3$</u> :



$\underline{p = 2:}$



(ii) f is Eisenstein for $p = 5$, so irreducible.

Let $L/\mathbb{Q}$ be the splitting field.

~~Let~~ Choose a prime $\mathfrak{p}$ over p, $\forall p$ primes of $\mathbb{Q}$, and let w be the extension of v_p to $L_{\mathfrak{p}}$.

$\underline{p = 5}$: $L_{\mathfrak{p}}$ contains elements α with $w(\alpha) = 1/5$ (roots of f) so

$$5 = e_{\mathbb{Q}_5(\alpha)|\mathbb{Q}_5} \mid e_{L_{\mathfrak{p}}|\mathbb{Q}_5} \Rightarrow$$

$$\Rightarrow 5 \mid [L : \mathbb{Q}].$$

Similarly $4 \mid [L:\mathbb{Q}]$ and $3 \mid [L:\mathbb{Q}]$ by choosing roots of f with ~~two~~ 2-adic valuation $1/4$ ~~and~~ resp 3-adic valuation $1/3$.

$\therefore \quad 60 \mid [L:\mathbb{Q}] \implies \mathrm{Gal}(L|\mathbb{Q}) = A_5$ or S_5.

To show that it's S_5, we need to show that the discriminant of f isn't a square in $\mathbb{Q}$.

We have $f(T) = T^5 + f'(T)$.

If $\alpha_1, \dots, \alpha_5$ are the roots of f, then

$$\operatorname{disc} f = \pm \prod_{i \neq j} (\alpha_i - \alpha_j) =$$

$$= \pm \prod_{i=1}^{5} \prod_{i \neq j} (\alpha_i - \alpha_j) = \pm \prod_{i=1}^{5} f'(\alpha_i) =$$

$$= \pm \prod_{i=1}^{5} \alpha_i^5 = \pm \left(\prod_{i=1}^{5} \alpha_i \right)^5 = \pm (5!)^5$$

which is not a square (~~divisible~~

$v_5((5!)^5) = 5$)

8. We have

$$\sum_i w(\alpha-\beta_i) = w\left(\prod_i (\alpha-\beta_i)\right) =$$

$$= w\Big(g(\alpha) - f(\alpha)\Big) =$$

$$= w\left(\sum_{j=0}^{n-1} (b_j - a_j)\alpha^i\right) \geq$$

$$\geq \min_{j=0,\dots,n-1} \Big(w(b_j - a_j) + i\,w(\alpha) \Big)$$

If $\quad w(\alpha-\beta_i) < \min\limits_{j=0,\dots,n-1} \left(\dfrac{w(b_j-a_j)}{n} + \dfrac{i\,w(\alpha)}{n} \right)$

$\forall i$, this would be a contradiction.

9. $w(\alpha - \sigma(\alpha)) = w(\alpha - \beta + \beta - \sigma(\alpha)) =$

$= w(\alpha - \beta + \sigma(\beta) - \sigma(\alpha))$ (since $\sigma(\beta) = \beta$) $=$

$= w(\alpha - \beta + \sigma(\beta - \alpha)) \geq$

$\geq \min\big(w(\alpha - \beta),\ w(\sigma(\alpha - \beta)) \big) =$

$= w(\alpha - \beta)$

since σ preserves valuations.

It follows that

$$w(\alpha - \sigma(\alpha)) > w(\alpha - \alpha_i) \quad \forall i \geq 2$$

But $\sigma(\alpha)$ is a $K(\beta)$-conjugate of α, hence a K-conjugate of α, so

$\sigma(\alpha) \in \{\alpha_1, \dots, \alpha_n\} \Rightarrow$

$\Rightarrow$ must have $\sigma(\alpha) = \alpha \quad \forall \sigma \in Gal(L/K(\beta))$

$\Rightarrow \alpha \in K(\beta)$, i.e. $K(\alpha) \subseteq K(\beta)$.

10. Let α be a primitive element of $L|\mathbb{Q}_p$. Fix an algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$ containing L.

Put $n = [L : \mathbb{Q}_p]$ and let $\alpha_2, \ldots, \alpha_n \in \overline{\mathbb{Q}_p}$ be the $\mathbb{Q}_p$-conjugates of α.

Let $f(T) \in \mathbb{Q}_p[T]$ be the min poly of $\alpha / \mathbb{Q}_p$.

Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, $\exists$ monic degree n polynomial $g(T) \in \mathbb{Q}[T]$ with a root $\beta \in \overline{\mathbb{Q}_p}$ s.t

$w(\alpha - \beta) > w(\alpha - \alpha_i)$

$\forall i \geq 2$, where w is the extension of v_p to $\overline{\mathbb{Q}_p}$. (use Q8 on this sheet)

By Krasner's Lemma (Q9)

$L = \mathbb{Q}_p(\alpha) \subseteq \mathbb{Q}_p(\beta)$.

Since $\deg g = n$, $[\mathbb{Q}_p(\beta) : \mathbb{Q}_p] \leq n =$

$= [L : \mathbb{Q}_p] \implies L = \mathbb{Q}_p(\beta)$

and g is irreducible over $\mathbb{Q}_p$, hence

over $\mathbb{Q}$.

Put $K = \mathbb{Q}(\beta)$; thus is an ext^n of

$\mathbb{Q}$ of degree n.

$$\text{Since } K = \bigoplus_{i=0}^{n-1} \mathbb{Q}\beta^i \subseteq \bigoplus_{i=0}^{n-1} \mathbb{Q}_p \beta^i = L,$$

we see that K is dense in L.

We may restrict v_L to K and we see

L is the completion of K with respect

to v_L.

To finish, we need to show that

v_L is equivalent to $v_{\mathfrak{p}}$ for some prime $\mathfrak{p} \subseteq \mathcal{O}_K$

containing p.

Now $~~v_L(\ldots)~~ - v_L(n) \geq 0 \ \forall n \in \mathbb{Z}$,

so since $\mathcal{O}_K$ is integral over $\mathbb{Z}$ we have $v_L(x) \geq 0 \ \forall x \in \mathcal{O}_K$.

$v_L|_{\mathbb{Q}} = e_{L|\mathbb{Q}_p} v_p$, so v_L is non-trivial

$$\Rightarrow \mathfrak{p} = \{x \in \mathcal{O}_K \mid v_L(x) > 0\}$$

is a maximal ideal containing p.

Let $\mathcal{O}_{K,\mathfrak{p}}$ be the localisation of $\mathcal{O}_K$ at $\mathfrak{p}$ (not its completion). Then $v_L(x) \geq 0$ $\forall x \in \mathcal{O}_{K,\mathfrak{p}}$. But we also have $v_{\mathfrak{p}}(x) \geq 0 \ \forall x \in \mathcal{O}_{K,\mathfrak{p}}$ ~~and~~.

By the ~~note~~ "Note" in the solution to Q13, Sheet 1, v_L and $v_{\mathfrak{p}}$ are equivalent, as desired, using that $\mathcal{O}_{K,\mathfrak{p}}$ is ~~[illegible]~~, a PID with a single prime, so it has ~~to~~ one non-negative valuation up to equivalence.

11. $$9f(T) = 27T^3 + 9T + 27 =$$
$$= (3T)^3 + 3(3T) + 27 =$$
$$= \cancel{g(3T)}\ g(3T)$$
where $g(T) = T^3 + 3T + 27$.

We work with g; $K = \mathbb{Q}(\alpha) = \mathbb{Q}(3\alpha)$ and 3α is a root of g.

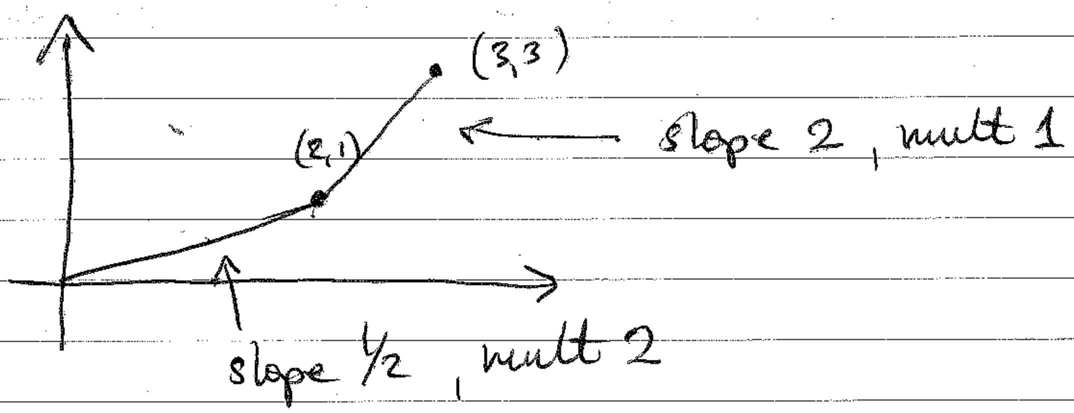
$$g(T) \equiv T^3 + T + 1 \mod 2$$

which is irreducible mod 2, so $g(T)$ is irreducible in $\mathbb{Q}_2$, hence in $\mathbb{Q}$.

This also shows that there is exactly one prime in $\mathcal{O}_K$ above 2.

For $p = 3$, draw the Newton polygon

Over $\mathbb{Q}_3$:



By Q5 we see that $g(T) = h_1(T)\,h_2(T)$ with h_1 quadratic irreducible and h_2 linear in $\mathbb{Q}_3[T]$ $\Rightarrow$ $\exists$ exactly two primes in $\mathcal{O}_K$ above 3.

For $p=5$, we check that $g(T)$ has no root mod 5 $\Rightarrow$ $g(T)$ irreducible in $\mathbb{Q}_5$, so $\exists$ exactly one prime above 5 in $\mathcal{O}_K$.

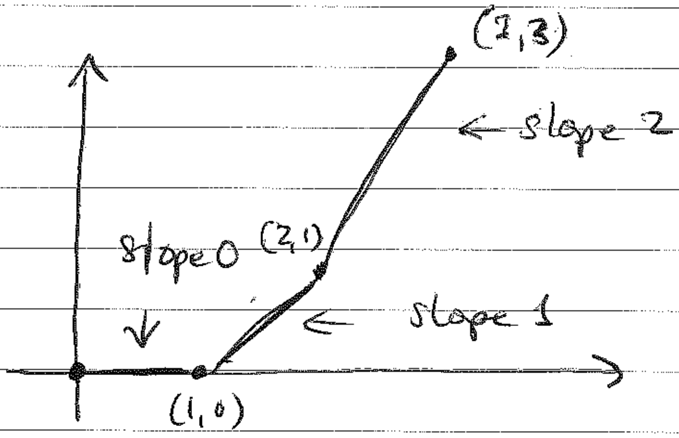
$$f(T) = T^3 + T^2 - 2T + 8.$$

12. f has no roots mod 3, so

f is irreducible $\Rightarrow$ $[K:\mathbb{Q}] = 3$.

The 2-adic Newton polygon of

$T^3 + T^2 - 2T + 8$ is



so $f(T)$ splits into linear factors in

$\mathbb{Q}_2[T]$ by Q5, so $\exists$ three distinct primes

of $\mathcal{O}_K$ above 2. $\Rightarrow$ $\exists$ three distinct

homomorphisms $\mathcal{O}_K \longrightarrow \mathbb{F}_2$

(one for each prime, the kernel being

that prime).

If $\mathcal{O}_K = \mathbb{Z}[\gamma]$, then any homomorphism

$G_K \to \mathbb{F}_2$ is determined by the image of γ and there are ≤ 2 possibilities since $\# \mathbb{F}_2 = 2$, so $\exists \leq 2$ homomorphism $G_K \to \mathbb{F}_2$ $\#$.

$\therefore$ there is no γ s.t $G_K = \mathbb{Z}[\gamma]$.

13. This is a sketch. You can also look at last years solution *

~~13a~~ Any automorphism σ of $\mathrm{Gal}(L|K)$ lifts to an automorphism $\sigma' \in S_n$ of $K[T_1, \dots, T_n]$ permuting the T_i ~~and~~, ~~which~~ satisfying

$$\sigma'(I) = I.$$

Conversely, any such automorphism induces an automorphism of the quotient $K[T_1, \dots, T_n]/I$

* Local Fields course on my webpage, Sheet 4, Q14, Solutions.

Next part:

Let $I = \mathrm{Ker}\left(\mathbb{Q}[T_1,\dots,T_n] \longrightarrow \mathbb{Q}(\alpha_1,\dots,\alpha_n)\right)$,

$J = \mathrm{Ker}\left(\mathbb{Q}_p[T_1,\dots,T_n] \longrightarrow \mathbb{Q}_p(\alpha_1,\dots,\alpha_n)\right)$

Then $I = J \cap \mathbb{Q}[T_1,\dots,T_n]$.

If $\sigma \in S_n$ it follows that

$$\sigma(J) = J \implies \sigma(I) = \sigma(J) \cap \sigma(\mathbb{Q}[T_1,\dots,T_n]) =$$
$$= J \cap \mathbb{Q}[T_1,\dots,T_n] = I$$

so $\mathrm{Gal}(f/\mathbb{Q}_p) \leq \mathrm{Gal}(f/\mathbb{Q})$.

Let $K = \mathbb{Q}(\alpha_1,\dots,\alpha_n) \subseteq L = \mathbb{Q}_p(\alpha_1,\dots,\alpha_n) \subseteq \overline{\mathbb{Q}_p}$

Restrict the ext^n w of v_p to $\overline{\mathbb{Q}_p}$ to K, then $w|_K$ is equivalent to $v_{\mathfrak{p}}$ for some $\mathfrak{p} \subseteq \mathcal{O}_K$ prime. (by the solution Q10), and L is the completion of K wrt $v_{\mathfrak{p}}$.

Thus $Gal(L|\mathbb{Q}_p) = D_{\mathfrak{P}|p} \subseteq Gal(K|\mathbb{Q})$.

~~Recall~~ Now assume f monic $\in \mathbb{Z}[T]$, seperable mod p. Let $\overline{\alpha}_1, \dots, \overline{\alpha}_n \in k_L$ ($=$ residue field of L) be the reductions of $\alpha_1, \dots, \alpha_n$; these are the roots of $\overline{f}$ and they are distinct; this gives the bijection.

We know from lectures that reduction gives an isomorphism $Gal(f/\mathbb{Q}_p) \xrightarrow{\sim} Gal(\overline{f}/\mathbb{F}_p)$ compatible with permuting the roots.

This gives the identification $Gal(f|\mathbb{Q}_p) = Gal(\overline{f}|\mathbb{F}_p)$ as permutation gps.

<u>Last part</u>: One checks that $f(T)$ is irreducible mod 2. The easiest way is

probably to prove that there are no solutions in $\mathbb{F}_4$ or $\mathbb{F}_8$, rather than trying to factor by brute force.

One checks that

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

again, by finding a root in $\mathbb{F}_9$. One then checks that $T^5-T^4-T^3-T+1$ has no roots in $\mathbb{F}_9$, so it's irreducible over $\mathbb{F}_3$.

By the previous part, $Gal(f/\mathbb{Q})$ contains a permutation σ of cycle type $(2,5)$. σ^2 is then a 5-cycle.