Homework 3

Songyu Ye

September 20, 2025

Problem 4 was written up with the help of ChatGPT. I believe I understand the correspondence but I had a hard time writing down why the constructions are inverses of each other.

Problem 1 Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p-th root of unity. Set $A = \mathbb{Z}$. Let B be the integral closure of A in L.

1. Prove that
$$(p) = \prod_{i=1}^{p-1}(1 - \zeta_p^i).$$

2. Show that $(p) = (1 - \zeta_p)^{p-1}$ as ideals of B. Deduce that (p) is totally ramified in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ (Recall that totally ramified in this context means that the ramification index is equal to the degree of the extension).

Solution:

1. Recall the p-th cyclotomic polynomial
$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1} = \prod_{i=1}^{p-1}(x - \zeta^i)$$
where ζ is a primitive p-th root of unity. Evaluate $\Phi_p(x)$ at $x = 1$:
$$\Phi_p(1) = 1 + 1 + \cdots + 1 = p$$
On the other hand,
$$\Phi_p(1) = \prod_{i=1}^{p-1}(1 - \zeta^i)$$
Therefore, in the ring $B \subset L$,
$$p = \prod_{i=1}^{p-1}(1 - \zeta^i)$$
which implies the equality on the level of ideals.

2. For any a with $1 \le a \le p - 1$, $1 - \zeta^a = (1 - \zeta)(1 + \zeta + \cdots + \zeta^{a-1})$, so $(1 - \zeta)$ divides $(1 - \zeta^a)$.

Since $\gcd(a,p)=1$, pick $b \in \{1,\dots,p-1\}$ with $ab \equiv 1 \pmod p$. Because $\zeta^p = 1$, we have $\zeta = \zeta^{ab}$. Thus

$$1-\zeta \;=\; 1-(\zeta^a)^b \;=\; (1-\zeta^a)\left(1+\zeta^a+\cdots+(\zeta^a)^{b-1}\right)$$

So $(1-\zeta^a)$ divides $(1-\zeta)$. This shows that $(1-\zeta^a)$ and $(1-\zeta)$ generate the same ideal in B.

Therefore,

$$(p) = \prod_{i=1}^{p-1}(1-\zeta^i) = (1-\zeta)^{p-1}$$

This shows that the ramification index is $p-1$, which is equal to the degree of the extension. Therefore, (p) is totally ramified in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

Problem 2 Keep using the notation from Problem 1.

1. For all positive integers i, prove that
$$B = \mathbb{Z}[\zeta_p] + (1-\zeta_p)^i B.$$

2. Show that
$$p^m B \subset \mathbb{Z}[\zeta_p]$$
for some positive integer m.

3. Conclude from (1) and (2) that $B = \mathbb{Z}[\zeta_p]$.

Solution:

1. It is enough to check that the equality holds at every localization at a prime ideal $\mathfrak{q}$ of B. Let $\pi = 1-\zeta$ and $\mathfrak{p} = (\pi)$ be the prime ideal above p. Then π is a uniformizer of the discrete valuation ring $B_{\mathfrak{p}}$, and the residue field $B_{\mathfrak{p}}/\mathfrak{p} \cong \mathbb{F}_p$ (because $ef = n$ and we showed above that $e = n$).

   Suppose $\mathfrak{q} \neq \mathfrak{p}$. Then π is a unit in $B_{\mathfrak{q}}$, so the equality holds trivially.

   Thus we need to check that
$$B_{\mathfrak{p}} = \mathbb{Z}[\zeta]_{\mathfrak{p}} + (1-\zeta)^i B_{\mathfrak{p}}$$
   for all $i \geq 1$. Consider the inclusion of $\mathbb{Z}[\zeta]_{\mathfrak{p}}$ into $B_{\mathfrak{p}}$ followed by the quotient map to the residue field:
$$\begin{aligned} \mathbb{Z}[\zeta]_{\mathfrak{p}} &\to B_{\mathfrak{p}}/\mathfrak{p} \cong \mathbb{F}_p \\ (a/s) &\mapsto a(1)/s(1) \mod p \end{aligned}$$

where we are thinking of

$$a = \sum_{k=0}^{p-2} a_k \zeta^k \in \mathbb{Z}[\zeta]$$
$$s = \sum_{k=0}^{p-2} s_k \zeta^k \in \mathbb{Z}[\zeta] \setminus \mathfrak{p}$$

where $s \notin \mathfrak{p}$ implies that $s(1) \not\equiv 0 \mod p$, and $f(1)$ means evaluating f at 1. This map is clearly a surjection between we can just choose a_k so that their sum is any element of $\mathbb{F}_p$, and then choose $s = 1$.

Now recall Nakayama's lemma: If M is a finitely generated module over a local ring R with maximal ideal $\mathfrak{m}$, and if a submodule $N \subseteq M$ maps surjectively onto the residue module $M/\mathfrak{m}M$, then $N = M$.

This implies that $\mathbb{Z}[\zeta]_{\mathfrak{p}} = B_{\mathfrak{p}}$ and therefore

$$B_{\mathfrak{p}} = \mathbb{Z}[\zeta]_{\mathfrak{p}} + \pi B_{\mathfrak{p}}$$

Multipling by π^{i-1} gives

$$B_{\mathfrak{p}} = \mathbb{Z}[\zeta]_{\mathfrak{p}} + \pi^i B_{\mathfrak{p}}$$

for all $i \geq 1$. This proves (1).

2. By the hint, it is enough to prove that $p^n \mathbb{Z}[\zeta]^* \subset \mathbb{Z}[\zeta]$ for some n. Let $e_i = \zeta^i$ be a basis of $\mathbb{Z}[\zeta]$ over $\mathbb{Z}$, and let f_i be the dual basis with respect to the trace form, i.e. $\mathrm{Tr}(e_i f_j) = \delta_{ij}$. Expand the f's in the e-basis:

$$f_i = \sum_j a_{ij} e_j, \quad a_{ij} \in \mathbb{Q}.$$

The matrix A is invertible. Define the matrix $G = (G_{ik})_{i,k}$, where

$$G_{ik} = \langle e_i, e_k \rangle = \mathrm{Tr}(e_i e_k)$$

Now compute

$$\begin{aligned}
\delta_{ij} &= \langle e_i, f_j \rangle \\
&= \left\langle e_i, \sum_k a_{kj} e_k \right\rangle \\
&= \sum_k a_{kj} \langle e_i, e_k \rangle \\
&= \sum_k G_{ik}\, a_{kj}.
\end{aligned}$$

which implies that $AG = I$. Thus $A = G^{-1}$. I claim that

$$G_{ij} = \begin{cases} p-1, & i+j \equiv 0 \pmod p, \\ -1, & \text{otherwise.} \end{cases}$$

where the indices i, j run from 0 to $p-2$. I also claim that from this computation one gets that $\det G = \pm p^{p-2}$. For the moment suppose that we have these two claims. Now observe that $G^{-1} = \frac{1}{\det G}\operatorname{adj}(G)$. Since $\operatorname{adj}(G)$ has integer entries, all denominators in G^{-1} divide $\det G$. Thus $M^* \subset \frac{1}{\det G}M$, i.e. $|(\det G)|M^* \subset M$ as desired.

It remains to prove the two claims about G. For the first claim, we have to show that

$$\operatorname{Tr}(\zeta^i\zeta^j) = \begin{cases} p-1, & i+j \equiv 0 \pmod p, \\ -1, & \text{otherwise.} \end{cases}$$

Let X be the linear operator on L defined by multiplication by ζ, and let s_i be the sequence of numbers $\operatorname{Tr}(X^i)$. Then $s_0 = p-1$ is clear. To calculate s_i for $1 \le i \le p-1$, note that the trace is going to be equal to coefficient of ζ^j in $\zeta^i\zeta^j = \zeta^{i+j}$ summed over $j = 1, \ldots, p-1$. These coefficients are all zero except in one instance when we have $i + j \cong p-1$, in which case the coefficient is -1 because we have to expand using the relation. Thus $s_i = -1$ for $1 \le i \le p-1$.

To compute the determinant of G, recall that we can add multiples of one column to another without changing the determinant. We will demonstrate the $p = 5$ case, which will hopefully illustrate the general case. The matrix is

$$G = \begin{pmatrix} 4 & -1 & -1 & -1 \\ -1 & -1 & -1 & 4 \\ -1 & -1 & 4 & -1 \\ -1 & -1 & -1 & -1 \end{pmatrix}$$

Subtracting the second column from the first, third, and fourth columns gives

$$G \sim \begin{pmatrix} 5 & -1 & 0 & 0 \\ 0 & -1 & 0 & 5 \\ 0 & -1 & 5 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

and one can quickly check that expanding along the first column gives $\det G = \pm 5^3$. The general case is similar, and one gets $\det G = \pm p^{p-2}$.

3. Let $A := B/\mathbb{Z}[\zeta_p]$. We have $B = \mathbb{Z}[\zeta_p] + (1-\zeta_p)^i B$ for all $i \ge 1$. Mod $\mathbb{Z}[\zeta_p]$ this says $A = (1-\zeta_p)^i A$ for all $i \ge 1$. Take $i = p-1$. Recall that we have from the first problem that $(1-\zeta_p)^{p-1} \in pB$. Hence $A = (1-\zeta_p)^{p-1}A \subset pA$, so $A = pA$.

   We also have $p^m B \subset \mathbb{Z}[\zeta_p]$, i.e. $p^m A = 0$. But $A = pA$ implies $A = p^k A$ for all k. Taking $k = m$ gives $A = p^m A = 0$. Therefore $B/\mathbb{Z}[\zeta_p] = 0$, i.e. $B = \mathbb{Z}[\zeta_p]$ as desired.

Problem 3 Let d be a square-free number (positive or negative) such that $d \neq 1$ and $d \equiv 1 \pmod 4$. Give a numerical condition for each rational prime p to be split, inert, or ramified in $\mathbb{Q}(\sqrt{d})$.

Solution: Recall the Dedekind-Webber theorem.

Theorem 0.1 (Dedekind-Webber)**.** *Let K be a number field and $\mathcal{O}_K$ the ring of algebraic integers in K. Let $\alpha \in \mathcal{O}_K$ and let f be the minimal polynomial of α over $\mathbb{Z}[x]$. For any prime p not dividing the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ of the free $\mathbb{Z}[\alpha]$-module $\mathcal{O}_K$, write*

$$f(x) \equiv \pi_1(x)^{e_1} \cdots \pi_g(x)^{e_g} \pmod p,$$

where $\pi_i(x)$ are monic irreducible polynomials in $\mathbb{F}_p[x]$. Then the ideal $(p) = p\mathcal{O}_K$ factors into prime ideals as

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

where the residue field degrees satisfy

$$N(\mathfrak{p}_i) = p^{\deg \pi_i},$$

and N denotes the ideal norm.

We have $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ because $d \equiv 1 \pmod 4$. The minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is $f(x) = x^2 - x + \frac{1-d}{4}$. The index $[\mathcal{O}_K : \mathbb{Z}[\frac{1+\sqrt{d}}{2}]] = 1$, so the Dedekind-Webber theorem applies to all primes. Now consider an odd prime p. Recall a double root occurs if and only if f and f' share a root mod p. Here $f'(x) = 2x - 1$. So a common root would be $x \equiv \frac{1}{2} \pmod p$; evaluate: $f\left(\frac{1}{2}\right) = \frac{1}{4} - \frac{1}{2} + \frac{1-d}{4} = -\frac{d}{4}$. Thus $f(\frac{1}{2}) \equiv 0 \pmod p$ if and only if $p \mid d$. Hence p is ramified if and only if $p \mid d$.

Now let p be an odd prime not dividing d. Then we can write

$$4f(x) = (2x-1)^2 - d.$$

Over $\mathbb{F}_p$, f has a root iff $(2x-1)^2 \equiv d$, i.e. iff d is a square mod p. Therefore p is split if d is a square mod p and p is inert if d is not a square mod p.

Finally consider the prime $p = 2$. Reduce f mod 2: $f(x) \equiv x^2 - x + \frac{1-d}{4} \pmod 2$. Now $\frac{1-d}{4} \equiv 0$ or $1 \pmod 2$. If $d \equiv 1 \pmod 8$: $f(x) \equiv x^2 - x = x(x-1)$ splits, so 2 splits. If $d \equiv 5 \pmod 8$: $f(x) \equiv x^2 - x + 1 = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, so 2 is inert. Also $f'(x) = 2x - 1 \equiv 1 \pmod 2$ never vanishes, so no double root. In particular, 2 does not ramify.

Problem 4 Let A be a Dedekind domain and K its fraction field. Show that the following two sets are in bijection:

1. The set of nonzero prime ideals $\mathfrak{p}$ of A.

2. The set of discrete valuations v on K which have nonnegative values on A,

via $\mathfrak{p} \mapsto v_{\mathfrak{p}}$ and $v \mapsto \mathfrak{p}_v := \{a \in A : v(a) > 0\}$.

Solution: Let $\mathfrak{p} \neq (0)$ be a prime of A. Since A is Dedekind, the localization $A_{\mathfrak{p}}$ is a discrete valuation ring (DVR) with maximal ideal $\mathfrak{m}_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$. Choose a uniformizer $\pi \in \mathfrak{m}_{\mathfrak{p}}$ so that $\mathfrak{m}_{\mathfrak{p}} = (\pi)$.

Define $v_{\mathfrak{p}} : K^\times \to \mathbb{Z}$ by: for $x \in K^\times$ write uniquely $x = u\pi^n$ with $u \in A_{\mathfrak{p}}^\times$ and $n \in \mathbb{Z}$, and set $v_{\mathfrak{p}}(x) = n$ (and $v_{\mathfrak{p}}(0) = +\infty$). This is a discrete valuation; moreover $v_{\mathfrak{p}}(a) \geq 0$ for every $a \in A$ (since $A \subset A_{\mathfrak{p}}$). Finally,

$$\mathfrak{p}_{v_{\mathfrak{p}}} = \{a \in A : \ v_{\mathfrak{p}}(a) > 0\} = \{a \in A : \ a \in \mathfrak{m}_{\mathfrak{p}} \cap A\} = \mathfrak{p}.$$

Let v be a nontrivial discrete valuation on K with $v(A) \geq 0$. Let

$$\mathcal{O}_v := \{x \in K : \ v(x) \geq 0\}, \qquad \mathfrak{m}_v := \{x \in K : \ v(x) > 0\}$$

be its valuation ring and maximal ideal. Then $\mathcal{O}_v$ is a DVR with fraction field K. Since $v(A) \geq 0$, we have an inclusion $A \subset \mathcal{O}_v$ and the contraction $\mathfrak{p}_v := A \cap \mathfrak{m}_v = \{a \in A : \ v(a) > 0\}$ is a nonzero prime of A.

Because $A \subset \mathcal{O}_v$ and elements of $A \backslash \mathfrak{p}_v$ have valuation 0, the universal property of localization yields a local injective ring map

$$\iota : A_{\mathfrak{p}_v} \hookrightarrow \mathcal{O}_v.$$

Both $A_{\mathfrak{p}_v}$ and $\mathcal{O}_v$ are DVRs with fraction field K. We claim ι is an isomorphism.

Let $\pi \in K^\times$ be a uniformizer for $\mathcal{O}_v$, so $v(\pi) = 1$ and $\pi\mathcal{O}_v = \mathfrak{m}_v$. In any DVR R with valuation w, one has $xR = \mathfrak{m}_R^{w(x)}$ for $x \in K^\times$. Apply this in $R = \mathcal{O}_v$:

$$\pi\, \mathcal{O}_v = \mathfrak{m}_v. \tag{$*$}$$

Write in $A_{\mathfrak{p}_v}$:

$$\pi\, A_{\mathfrak{p}_v} = \mathfrak{m}_{\mathfrak{p}_v}^n, \qquad n := v_{\mathfrak{p}_v}(\pi) \in \mathbb{Z}_{\geq 1},$$

where $v_{\mathfrak{p}_v}$ is the normalized valuation of the DVR $A_{\mathfrak{p}_v}$ and $\mathfrak{m}_{\mathfrak{p}_v} = \mathfrak{p}_v A_{\mathfrak{p}_v}$. Extending ideals from $A_{\mathfrak{p}_v}$ to $\mathcal{O}_v$ (through ι) gives

$$\pi\, \mathcal{O}_v \ = \ (\pi\, A_{\mathfrak{p}_v})\, \mathcal{O}_v \ = \ \big(\mathfrak{m}_{\mathfrak{p}_v} \mathcal{O}_v\big)^n.$$

Comparing with ($*$) and using that powers of the unique maximal ideal of a DVR are strictly decreasing, we deduce

$$\mathfrak{m}_{\mathfrak{p}_v} \mathcal{O}_v = \mathfrak{m}_v \qquad \text{and} \qquad n = 1.$$

Hence the local map ι identifies the maximal ideals and sends a uniformizer of $A_{\mathfrak{p}_v}$ to a uniformizer of $\mathcal{O}_v$; therefore ι is an isomorphism of DVRs. In particular the induced valuations agree on K:

$$v_{\mathfrak{p}_v} = v.$$