Berkeley Math 254A
Algebraic Number Theory

Solved Problem Sets

Javier López-Contreras

Fall 2022

HW1. September 7th

Problem 1.1. *Let D be a square-free integer. Show that the ring of integers of $\mathbb{Q}(\sqrt{D})$ is equal to $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ if $D \equiv 1 \pmod 4$ and $\mathbb{Z}[\sqrt{D}]$ otherwise.*

Solution.

- Take a base of $\mathbb{Q}(\sqrt{D})$, namely $e_1 = 1$ and $e_2 = \sqrt{D}$. In such base, the multiplication map of a generic element $\zeta = a + b\sqrt{D}$ is
$$\begin{pmatrix} a & bD \\ b & a \end{pmatrix}$$
,
so its trace and norm are $\mathrm{Tr}(\zeta) = 2a$ and $\mathrm{Nm}(\zeta) = a^2 - b^2D$.
- For ζ to be in the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, its trace and norm must be in $\mathbb{Z}$. In quadratic extensions, this condition also suffices as the minimal polynomial of any element will be of degree at most 2, so its only coefficients will be 1, the trace and the norm.
- Let $a = \frac{x}{2}$ and $b = \frac{y}{z}$ with $x, y, z \in \mathbb{Z}$ and $(y, z) = 1$. Then, $a^2 - b^2D = k$ iff
$$x^2z^2 - 4y^2D = 4z^2k$$
- Looking $\pmod 4$, we get that either x or z are even.
- If x is even, a is an integer, so by the additivity of the integral elements, $b\sqrt{D}$ must be an integer as well. Hence, $\frac{y^2}{z^2}D \in \mathbb{Z}$, so $z^2|D$. But D is square-free, so $z = \pm 1$ and b is an integer. This shows that regardless of $D \pmod 4$, $\mathbb{Z}[\sqrt{D}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$
- Else, if x is odd and z is even, let $z = 2z'$. Then $x^2z'^2 - y^2D = 4z'^2k$. Looking $\pmod{z'^2}$, we get that $z'^2|y^2D \implies z'^2|D$ as $(y, z') = 1$. Because D is square-free, $z' = \pm 1$, so we can assume that $z = 2$.
- Finally $x^2 - y^2D = 4k$, with x odd. Looking $\pmod 4$, $y^2D \equiv 1 \pmod 4$. If $D \equiv 2, 3 \mod 4$, this case gives no extra solutions, so $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\sqrt{D}]$. But if $D \equiv 1 \pmod 4$, any y odd gives a solution $\frac{x+y\sqrt{D}}{2}$, hence $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$

Problem 1.2. *Consider the ring $A = \mathbb{C}[x, y]/(y^2 - x^2(x - 1))$. Show that A is an integral domain but it is not integrally closed in its field of fractions.*

Solution.

- The ring A is integral $\iff f(x, y) := y^2 - x^2(x - 1) = (y^2 + x^2) - x^3$ is irreducible. This follows from a general result stating that the sum of a n-th degree homogeneous polynomial and a $n + 1$-th degree homogeneus polynomial is always irreducible on $\mathbb{C}[x, y]$.
- Note that $A = \mathbb{C}[x, y]/(y^2 - x^2(x - 1)) = \mathbb{C}[x, x(x - 1)^{1/2}]$

- Hence, note that $K = \text{Frac}(A) = \mathbb{C}((x-1)^{1/2})$ as the other generator x is $x = ((x-1)^{1/2})^2 + 1$
- Let $f(T) = T^2 + T + \frac{x}{4}$, a monic polynomial with coefficients in A. One of it's roots, $\frac{-1+(1-x)^{1/2}}{2} \in K - A \iff (x-1)^{1/2} \in K - A$, which is true. Hence A is not integrally closed.

Problem 1.3. *Let K be a field of positive characteristic p and let $f \in K$ be an element which is not a p-th power. Let $L = K[x]/(x^p - f)$. Show that L is a field and describe the trace map* $\text{Tr} : L \to K$.

Solution.

- L is a field $\iff$ $f(x) = x^p - f$ is irreducible.
- In the algebraic closure $f(x)$ decomposes linearly and, since we are in characteristic p, it must do so in the form $f(x) = (x - \epsilon)^p$.
- Hence, if $f(x)$ was reducible in $F[x]$, there must be a $k < p$ such that $(x-\epsilon)^k$ is in $F[x]$.
- Expanding the binomial, we get that ϵ^k and $k\epsilon^{k-1}$ are in F. Since $k < p$ and a field is an integral domain, $k\epsilon^{k-1} \neq 0$. This implies that $\epsilon = k\epsilon^k/(k\epsilon^{k-1}) \in F$, which is a contradiction with $f(x)$ irreducible.
- We have seen that $f(x)$ is not separable so the trace can not be expressed as the sum of the Galois conjugates. We use the definition.
- Take a base in L, namely $\{1, x, \cdots, x^{p-1}\}$. An element on L $r(x) = a_0 + a_1 + \cdots a_{p-1}x^{p-1}$ has a multiplication representation
$$\begin{pmatrix} a_0 & a_{p-1}f & \cdots & a_1 f \\ a_1 & a_0 & \cdots & a_2 f \\ \vdots & \vdots & \ddots & \vdots \\ a_{p-1} & a_{p-2} & \cdots & a_0 \end{pmatrix}$$
- Hence, $\text{Tr} : L \to K, r(x) \mapsto p \cdot r(0) = 0$ is the constant function to zero.

Problem 1.4. *Let D and D' be distinct square free integers > 1. Show that $\mathbb{Q}(\sqrt{D})$ is not isomorphic to $\mathbb{Q}(\sqrt{D'})$.*

Solution.

- Suppose the contrary. Then there is an isomorphism $\phi : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}(\sqrt{D'})$.
- For all $q = \frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$, we have $\phi(q) = q$, as $\phi(a/b) = \phi(a)/\phi(b)$ and $\phi(a) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = a$
- Now, let $\phi(\sqrt{D}) = \gamma = a + b\sqrt{D'}$, with $a, b \in \mathbb{Q}$. Then, $\gamma^2 = \phi(\sqrt{D}^2) = D$.
- $\gamma^2 = a^2 + b^2D' + 2ab\sqrt{D'} = D$, so either a or b is 0. If $b = 0$, $\gamma^2 = a^2 = D$, which contradicts D square-free. Else, if $a = 0$, $\gamma^2 = b^2D' = D$, which, by D square free, means $b = \pm 1$, so either $D = D'$ or $D = -D'$, and both give contradictions of the assumed statement.

Problem 1.5. *Show that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain by showing that the ideal $(2, 1 + \sqrt{-5})$ is not principal.*

Solution.

- Suppose $(2, 1 + \sqrt{-5})$ was a principal ideal, generated by $\pi = c + d\sqrt{-5}$. Then, $2 = \pi s$ and $1 + \sqrt{-5} = \pi t$, with $s, t \in \mathbb{Z}[\sqrt{-5}]$
- Recall from Problem 1.1 that $\text{Nm}(a + b\sqrt{-5}) = a^2 + 5b^2$.
- Taking norms on the two equations above, $\text{Nm}(2) = 4 = \text{Nm}(\pi)\text{Nm}(s)$ and $\text{Nm}(1 + \sqrt{-5}) = 6 = \text{Nm}(\pi)\text{Nm}(t)$. We conclude that, since it is a common divisor of 4 and 6, $\text{Nm}(\pi) \in \{\pm 1, \pm 2\}$.

- $\mathrm{Nm}(\pi) = c^2 + 5d^2 \geq 0$ so the negative candidates are discarded. There are no integral solutions to $c^2 + 5d^2 = 2$, so the only possibility left to consider is $\mathrm{Nm}(\pi) = 1 \implies \pi$ is a unit, we may assume $\pi = 1$.
- $c^2 + 5d^2 = 1 \implies c = 1, d = 0 \implies \pi = 1$
- But $1 \notin (2, 1+\sqrt{-5})$ as if $1 = 2(a+b\sqrt{-5})+(1+\sqrt{-5})(c+d\sqrt{-5}) = (2a+c-5d)+\sqrt{-5}(2b+c+d) \implies$

$$1 = 2a + c - 5d$$
$$0 = 2b + c + d$$

  $\implies 2(a - b - 3d) = 1$, which has no integer solutions because of parity.
- Hence $\pi = 1 \notin (2, 1 + \sqrt{-5}) = (\pi)$, which is contradictory.

HW2. September 12th

Problem 2.1. *Let L/K be a finite separable extension of fields and let $K \to K^{\mathrm{sep}}$ be a separable closure of K. Show that the map*

$$L \otimes_K K^{\mathrm{sep}} \to \prod_{\sigma: L \hookrightarrow K^{\mathrm{sep}}} K^{\mathrm{sep}},\ l \otimes x \mapsto (x\sigma(l))_\sigma$$

is an isomorphism.

Solution.

- It is clear that the map is a morphism of K-vector spaces and is injective. To show surjectivity I will show that the map is between equal dimensional vector spaces.
- If L is a n-dimensional extension of K, we have the isomorphism of vector spaces $L \simeq K^n$. The tensor product commutes with the product, so $L \otimes_K K^{\mathrm{sep}} = \prod(K \otimes_K K^{\mathrm{sep}}) = \prod K^{\mathrm{sep}}$
- Finally, $n = |\{\sigma : L \hookrightarrow K^{\mathrm{sep}}\}|$ because the extension is separable.

Problem 2.2. *Let $A = \mathbb{Z}[\sqrt{-5}]$. Show that*

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

are two factorizations of 6 into irreducibles and therefore A is not a UFD. What is the factorization of the ideal (6) as product of prime ideals?

Solution.

- Recall from Problem 1.1 that $\mathrm{Nm}(a + b\sqrt{-5}) = a^2 + 5b^2$.
- Notice that for all $\zeta \in \{2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}\}$, their norms are $\mathrm{Nm}(\zeta) \in \{4, 9, 6\}$, which are all product of 2 primes. If any of these ζ is not irreducible, they would have a non-unit factor π with norm $\mathrm{Nm}(\pi) \in \{2, 3\}$. But $a^2+5b^2 = k$ has no integer solutions for $k \in \{2, 3\}$. This proves that all the ζ are irreducible elements.
- Nonetheless, they are not primes as ideals as, by the equality on the statement, each of the generated ideals by some ζ contains a product of two elements not in (ζ). For example, $2 \cdot 3 \in (1+\sqrt{-5})$ but neither of them is because $\mathrm{Nm}(1 + \sqrt{-5}) = 6 \not| 4 = \mathrm{Nm}(2)$. This happens for all pairings as none of the numbers $\{4, 6, 9\}$ divide each other.
- We claim that $\mathfrak{p}_1 = (2, 1 + \sqrt{-5}), \mathfrak{p}_2 = (3, 1 + \sqrt{-5}), \mathfrak{p}_3 = (2, 1 - \sqrt{-5}), \mathfrak{p}_4 = (3, 1 - \sqrt{-5})$ are all prime ideals in $\mathbb{Z}[\sqrt{-5}]$ and then, the descomposition above as ideals is

  $$(6) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4),$$

  which doesn't contradict uniqueness up to reordering.

- We first show that each $(\zeta) = \mathfrak{p}_i\mathfrak{p}_j$. The right to left inclusion is given by $\mathfrak{p}_i\mathfrak{p}_j \subseteq \mathfrak{p}_i \cap \mathfrak{p}_j = (\zeta)$, because of how the $\mathfrak{p}_i$ are defined. The other inclusion comes from the equations

$$\begin{aligned} 2 &= (1+\sqrt{-5})(1-\sqrt{-5}) - 2^2 \\ 3 &= -(1+\sqrt{-5})(1-\sqrt{-5}) + 3^2 \\ 1+\sqrt{-5} &= 3(1+\sqrt{-5}) - 2(1+\sqrt{-5}) \\ 1-\sqrt{-5} &= 3(1-\sqrt{-5}) - 2(1-\sqrt{-5}) \end{aligned}$$

- Lastly, note that $\mathfrak{p}_1 = (2, 1+\sqrt{-5}) = (2, 1-\sqrt{-5}) = \mathfrak{p}_3$, so the prime ideal decomposition of 6 has a ramification at $\mathfrak{p}_1 = \mathfrak{p}_3$.

Problem 2.3. [1, Ch.9, Ex.7] *Let A be a Dedekind domain and let $\mathfrak{a} \subseteq A$ be a nonzero ideal. Show that every ideal in $A/\mathfrak{a}$ is principal. Note that this implies that every ideal in a Dedekind domain is generated by two elements.*

Solution.

- By prime ideal factorization in a Dedekind domain A, $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. By the Approximation Lemma, $A/\mathfrak{a} = A/\mathfrak{p}_1^{e_1} \times \cdots \times A/\mathfrak{p}_r^{e_r}$.
- By the quotient structure, there is a bijection of

$$\{\text{ideals } I \in A/\mathfrak{a}\} \leftrightarrow \{\text{ideals } J \in A \text{ st } \mathfrak{a} \subseteq J (\iff J|\mathfrak{a})\}$$

  As A is a Dedekind domain, the ideals J in the right side can be characterized as $J = \mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_r^{d_r}$ with $0 \leq d_i \leq e_i$.
- Such an ideal J, under the bijection given by the Aprox. Lemma, is $J = \mathfrak{p}_1^{d_1} \times \cdots \times \mathfrak{p}_r^{d_r}$. Suppose π_i is a generator of $\mathfrak{p}_i^{d_i} \subseteq A/\mathfrak{p}_i^{e_i}$. Then J is generated by $(\pi_1, \cdots, \pi_r)$
- It remains to be proven that $A/\mathfrak{p}^n$ is PID. It is necessary and sufficient that $\mathfrak{p}$ is principal, as all other ideals are $\mathfrak{p}^k$. Note that $\mathfrak{p}^2 \subsetneq \mathfrak{p}$ as they are not equal in A. Hence, we can take $x \in \mathfrak{p} - \mathfrak{p}^2$ and consider the principal ideal (x) which must be one of the possible ideals $\mathfrak{p}^k$ but if $k \geq 2 \implies x \in \mathfrak{p}^k \subseteq \mathfrak{p}^2$, which contradicts the choice of x. Hence $(x) = \mathfrak{p}$, which proves that $A/\mathfrak{a}$ is PID.
- Take any ideal $I \subseteq A$ and any $a \neq 0, a \in I$. We know that $(a) \subseteq I$ is a non-zero ideal. Hence, I maps to some $I' \subseteq A/(a)$. By the proof above, I' is principal, say $I' = (b)$. Reversing the bijection, we get $I = (b) + (a) = (a, b)$.

Problem 2.4. *Fix a prime p. Viewing $\mathbb{Q}$ as the field of fractions of the discrete valuation ring $\mathbb{Z}_{(p)}$ we have the p-adic valuation*

$$\nu_p : \mathbb{Q} \to \mathbb{Z}$$

Define

$$|\cdot|_p : \mathbb{Q}^* \to R$$

by the formula

$$|x|_p := \frac{1}{p^{\nu_p(x)}}$$

We extend this to all of $\mathbb{Q}$ with the convention that $|0|_p = 0$.

1. *Show that $|\cdot|_p$ satisfies the axioms for a norm:*
   (a) $|0|_p = 0$
   (b) $|xy|_p = |x|_p|y|_p$
   (c) $|x+y|_p \leq |x|_p + |y|_p$

2. *(Product formula) Show that for $x \in \mathbb{Q}$ we have*

$$1 = \prod_p |x|_p$$

where on the right the product is taken over all prime numbers p as well as $p = \infty$, where by convention $|\cdot|_\infty$ us guven by the usual absolute value on $\mathbb{R}$. Note here that some care should also be taken to explain why this infinite product makes sense.

Solution.

1. For this section, we will use the notation $p^n||x$ with p prime, $x = a/b \in Q^*$ to indicate $n = \nu_p(a) - \nu_p(b)$.
   - a) is true by definition
   - b) is equivalent to $\nu_p(xy) = \nu_p(x) + \nu_p(y)$. If $p^n||x$ and $p^m||y$ then $p^{n+m}||xy$.
   - c) is implied by $\nu_p(x+y) \leq \min\{\nu_p(x), \nu_p(y)\}$. This is because if $p^n||x$ and $p^m||y$, we may assume $n \leq m$, then $x + y = p^n(u + p^{m-n}v)$ and this is divisible at least n times by p. If $m \neq n$, this will be divisible exactly n times by p as the other factor will be u, which is not divisible by p.
2. Let $x = \text{sign}(x) \prod_{p \in \mathbb{Z}} p^{\nu_p(x)}$ be the usual prime decomposition in $\mathbb{Q}$
   - Notice that this product only runs over a finite number of primes, those that divide either the numerator or denominator of x.
   - The product on the statement only runs for the primes defined above and the one at infinity, so it can be considered a finite product. For any other prime q, $|x|_q = q^{-v_q(x)} = q^0 = 1$.
   - Now, notice that $|x|_\infty = \prod_{p \in \mathbb{Z}} p^{\nu_p(x)}$ and that $|x|_p = p^{-\nu_p(x)}$, so multiplying all the terms together cancels all the exponents, ending in 1.

Problem 2.5. [4, Ch.II, §2, Ex. 2] *Let n be a natural number and let p be a prime*

1. *Show that we can write n uniquely as*

$$n = a_0 + a_1 p + \cdots + a_{r-1} p^{r-1}$$

with $0 \leq a_i < p$.

2. *Let s denote $a_0 + a_1 + \cdots + a_{r-1}$. Show that*

$$\nu_p(n!) = \frac{n - s}{p - 1}$$

.

Solution.

1. - We can show existence inductively. For $0 \leq n < p$, the statement is trivial letting $r = 1$, $a_0 = n$. For other n, by integer division we can express $n = mp + t$ and following by induction in $m < n$, $m = b_0 + \cdots b_{l-1} p^{l-1}$. Now we can set $r = l + 1$, $a_i = b_{i-1}$ for $i > 0$ and $a_0 = t$ which gives us a valid base extension.
   - We can also show uniqueness by finite induction on the number of digits. Suppose we have two such expressions, $n = a_0 + \cdots$ and $n = b_0 + \cdots$ then, $n - n = 0 = a_0 - b_0 \pmod p$, so $a_0 = b_0 \mod p$ and because they are $0 \leq a_0, b_0 < p$, we have $a_0 = b_0$. Now we can proceed (finitely) inductively on $(n - a_0)/p < n$. The number of digits will go to zero in finite steps, so we don't really need the inductive axiom.

2.

$$\begin{aligned}
\nu_p(n!) = \sum_{i=1}^{n} \nu_p(n) &= \sum_{i=1 \text{ st } p|i} 1 + \sum_{i=1 \text{ st } p^2|i} 1 + \cdots \\
&= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^{r-1}} \right\rfloor \\
&= (a_1 + \cdots + a_{r-1}p^{r-2}) + (a_2 + \cdots + a_{r-1}p^{r-3}) + \cdots + a_{r-1} \\
&= a_1 + a_2(p+1) + \cdots + a_{r-1}(p^{r-2} + \cdots + 1) \\
&= a_1 \frac{p-1}{p-1} + a_2 \frac{p^2-1}{p-1} + \cdots + a_{r-1} \frac{p^{r-1}-1}{p-1} \\
&= \frac{a_0 + \cdots a_{r-1}p^{r-1} - a_0 - \cdots - a_{r-1}}{p-1} \\
&= \frac{n-s}{p-1}
\end{aligned}$$

HW3. September 19th

Problem 3.1. [4, Ch.I, §2, p.15, Ex. 4, 5, 6, 7]

4. *Let D be a square-free rational integer $\neq 0, 1$ and d the discriminant of the quadratic number field $K = \mathbb{Q}(\sqrt{D})$. Show that*

$$\begin{aligned}
d = D, \text{ if } D \equiv 1 \mod 4 \\
d = 4D, \text{ if } D \equiv 2, 3 \mod 4
\end{aligned}$$

and that an integral basis of K is given by $\{1, \sqrt{D}\}$ in the second case, by $\{1, \frac{1}{2}(1+\sqrt{D})\}$ in the first case, and by $\{1, \frac{1}{2}(d+\sqrt{d})\}$ in both cases.

5. *Show that $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$ is an integral basis of $\mathbb{Q}(\sqrt[3]{2})$.*

6. *Show that $\{1, \theta, \frac{1}{2}(\theta + \theta^2)\}$ is an integral basis of $\mathbb{Q}(\theta)$, $\theta^3 - \theta - 4 = 0$.*

7. *The discriminant d_K of an algebraic number field K is always $\equiv 0, 1 \mod 4$ (Stickelberger's discriminant relation)*

   Hint: *The determinant $\mathrm{Det}(\sigma_i w_j)$ of an integral basis w_j is a sum of terms, each prefixed by a positive or negative sign. Writing P, resp. N, for the sum of the positive, resp. negative, terms, one finds $d_K = (P-N)^2 = (P+N)^2 - 4PN$*

Solution.

4.
- We proved the integral basis of the quadratic field in Problem 1.1. Recall from that same problem that $\mathrm{Tr}(a + b\sqrt{D}) = 2a$
- Using these basis, the discriminant can be computed as the determinant of the trace pairing matrix.
  - $\boxed{D \equiv 1 \mod 4}$. The trace pairing matrix is

$$\begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}\left(\frac{1}{2}(1+\sqrt{D})\right) \\ \mathrm{Tr}\left(\frac{1}{2}(1+\sqrt{D})\right) & \mathrm{Tr}\left((\frac{1}{2}(1+\sqrt{D}))^2\right) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+D}{2} \end{pmatrix}$$

    Hence the discriminant is $d = D$.
  - Clearly $\{1, \frac{1}{2}(D+\sqrt{D})\}$ is a base as $\frac{1}{2}(1+\sqrt{D}) = \frac{1}{2}(D+\sqrt{D}) - \frac{D-1}{2}$ and $D-1$ is even.
  - $\boxed{D \equiv 2, 3 \mod 4}$. The trace pairing matrix is

$$\begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}\left(\sqrt{D}\right) \\ \mathrm{Tr}\left(\sqrt{D}\right) & \mathrm{Tr}\left(\sqrt{D^2}\right) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix}$$

    Hence the discriminant is $d = 4D$.

– Indeed $\{1, 2D + \sqrt{D}\}$ is a base as $\sqrt{D} = \sqrt{D} + 2D - 2D$.

5.
- Denote $K = \mathbb{Q}(\sqrt[3]{2})$. We have $\mathcal{R} = \mathbb{Z}[\sqrt[3]{2}, \sqrt[3]{2}^2] \subseteq \mathcal{O}$ by $T^3 - 2$ and $T^3 - 4$. Lets compute the determinant of $\mathcal{R}$, which will be an integer, by virtue of $\mathcal{R}$ being an extension of $\mathbb{Z}$.
- First, let's compute the trace explicitly on the base $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$. If $a + b\sqrt[3]{2} + c\sqrt[3]{2^2}$ is a generic element of K, it is represented as a matrix

$$\begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}$$

so $\mathrm{Tr}(a + b\sqrt[3]{2} + c\sqrt[3]{2^2}) = 3a$
- The trace pairing matrix is

$$\begin{pmatrix} \mathrm{Tr}\,(1) & \mathrm{Tr}\left(\sqrt[3]{2}\right) & \mathrm{Tr}\left(\sqrt[3]{2^2}\right) \\ \mathrm{Tr}\left(\sqrt[3]{2}\right) & \mathrm{Tr}\left(\sqrt[3]{2^2}\right) & \mathrm{Tr}\,(2) \\ \mathrm{Tr}\left(\sqrt[3]{2^2}\right) & \mathrm{Tr}\,(2) & \mathrm{Tr}\left(2\sqrt[3]{2}\right) \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{pmatrix}$$

so the determinant is $d_R = -3^3 2^2$.
- A priori, the determinant $d_{\mathcal{O}}$ can be either of $\{-3^1, -3^1 2^2, -3^3 2^2\}$.
- Because 2 ramifies as $2 = (\sqrt[3]{2})^3$, $2 | d_{\mathcal{O}}$ so the first option is discarded.
- Going to the completion at 3, $\mathbb{Q}_3(\sqrt[3]{2}) = \mathbb{Q}_3(\sqrt[3]{2}+1)$ and $(x-1)^3 - 2 = x^3 - 3x^2 + 3x - 3$ is Einsestein, so the extension is totally ramified, $e_3 = 3$. Also, $3|3$, we are not in the tamely ramified case, so the exponent in the discriminant must be $\geq e = 3$, hence the second case is discarded.

6. Very similar to 5 so I'll show the computations briefly
- $\mathbb{Z}[\theta, \frac{1}{2}(\theta + \theta^2)] \subseteq \mathcal{O}$ as $T^3 - T - 4$ has root θ and $T^3 - T^2 - 3T - 2$ has root $\frac{1}{2}(\theta + \theta^2)$. The latter polynomial was found computing the characteristic polynomial of the matrix representation below with $a = 0, b = 0, c = 1$.
- In this base, the matrix of $\zeta = a + b\theta + c\frac{1}{2}\theta(\theta + 1)$ is

$$\begin{pmatrix} a & 2c & 2b + 2c \\ b & a - b & c \\ c & 2b + c & a + b + c \end{pmatrix}$$

so its trace is $\mathrm{Tr}(\zeta) = 3a + c$
- Now, the discriminant is

$$\begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\theta) & \mathrm{Tr}(\frac{1}{2}\theta(\theta+1)) \\ \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) & \mathrm{Tr}(\frac{1}{2}\theta^2(\theta+1)) \\ \mathrm{Tr}(\frac{1}{2}\theta(\theta+1)) & \mathrm{Tr}(\frac{1}{2}\theta^2(\theta+1)) & \mathrm{Tr}(\frac{1}{4}\theta^2(\theta+1)^2) \end{pmatrix} =$$

$$\begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\theta) & \mathrm{Tr}(\frac{1}{2}\theta(\theta+1)) \\ \mathrm{Tr}(\theta) & \mathrm{Tr}(2(\frac{1}{2}(\theta^2+\theta)) - \theta) & \mathrm{Tr}(\frac{1}{2}\theta(\theta+1)+2) \\ \mathrm{Tr}(\frac{1}{2}\theta(\theta+1)) & \mathrm{Tr}(\frac{1}{2}\theta(\theta+1)+2) & \mathrm{Tr}(\frac{1}{2}\theta(\theta+1)+\theta+2) \end{pmatrix} = \begin{pmatrix} 3 & 0 & 1 \\ 0 & 2 & 7 \\ 1 & 7 & 7 \end{pmatrix}$$

Hence the discriminant is $d_R = -107$, which is a prime, hence square free. So $R = \mathcal{O}$.

7.
- Following the hint, let $\{w_1, \ldots, w_n\}$ an integral basis of L/K.
- Let $A = (\sigma_i w_i)$. We claim that $\mathrm{Det}(A) = P - N$ with $P, N > 0$ rational integers with

$$P = \sum_{\mu \in \mathrm{Sym}(n) \text{ with } \mathrm{sign}(\mu)=1} \prod_{i=0}^{n} \sigma_i(w_{\mu(i)})$$

- $\forall \zeta \in \mathrm{Gal}(K/\mathbb{Z})$, $\zeta = \sigma_j$ so

$$\zeta(P) = \sum_{\mu \in \mathrm{Sym}(n) \text{ with } \mathrm{sign}(\mu)=1} \prod_{i=0}^{n} \sigma_j(\sigma_i(w_{\mu(i)})) = \sum_{\mu \in \mathrm{Sym}(n) \text{ with } \mathrm{sign}(\mu)=1} \prod_{k=0}^{n} \sigma_k(w_{\mu(i)}) = P$$

since the action of σ_j in $\mathrm{Gal}(K/\mathbb{Z})$ is transitive. Hence $P \in \mathbb{Z}$ and, equivalently, $N \in \mathbb{Z}$.

- Then, the trace pairing matrix is $T = AA^T$ so $\text{Disc}_{L/K} = \text{Det}(T) = \text{Det}(A)^2 = (P-N)^2 = (P+N)^2 - 4NP$, which mod 4 is a square, hence its either 0 or 1.

Problem 3.2. *An integral domain A is called a **Euclidian domain** if it admits a function*

$$N : A - \{0\} \to \mathbb{N}$$

such that for any $a, b \in A$ with $b \neq 0$ there exist elements $s, t \in A$ such that

$$a = sb + t$$

*and either $t = 0$ or $N(t) < N(b)$. Informally, we have a division with reminder respect to the function N, which is sometimes called a **Euclidian function**.*

1. *Show that if A is a Euclidian domain then A is a PID.*
2. *Show that the function*
$$N : \mathbb{Z}[i] \to \mathbb{N}, a + bi \mapsto a^2 + b^2$$
is a Euclidian function, and therefore $\mathbb{Z}[i]$ has a trivial class group.
3. *Let ζ_3 be a primitive third root of unity. Explicitly we can take*
$$\zeta_3 = \frac{-1 + \sqrt{-3}}{2}$$
Consider the ring $\mathbb{Z}[\zeta_3]$, and show that the function
$$N : \mathbb{Z}[\zeta_3] - \{0\} \to \mathbb{Z}, a + b\zeta_3 \mapsto a^2 - ab + b^2$$
is an Euclidian function and therefore the class group of $\mathbb{Z}[\zeta_3]$ is trivial.

Solution.

1. - Take an arbitrary ideal $I \subseteq A$, and consider the set $N(I) \subseteq \mathbb{N}$, which is lower bounded by 0 and discrete hence it has a minimum. Denote π one of the elements that achieve the minimum.
   - For any other element $x \in I$, there are elements $s, t \in A$ such that $x = s\pi + b$ and either $b = 0$ or $N(b) < N(\pi)$.
   - In the latter, $b = x - s\pi \in I$ has smaller norm than π, which contradicts that π is minimal. Hence $b = 0$, so $x = s\pi$ and $I = (\pi)$.
2. - For any arbitrary $x = a + bi$ and $y = c + di$ in $\mathbb{Z}[i]$, let q_R, q_I, r_R, r_I be the quotient and residues of the integer divisor of $ac + bd$ and $bc - da$ by $c^2 + d^2$, such that
$$ac + bd = q_R(c^2 + d^2) + r_R, \;\; |N_{\mathbb{Z}}(r_R)| \leq \frac{1}{2}(c^2 + d^2)$$
$$bc - da = q_I(c^2 + d^2) + r_I, \;\; |N_{\mathbb{Z}}(r_I)| \leq \frac{1}{2}(c^2 + d^2)$$
   - Then, choose
$$s = q_R + iq_I, \;\; t = \frac{(r_R + ir_I)(c - di)}{c^2 + d^2} =$$
   - One can check that $a + bi = (c + di)s + t$ by construction, which implies that $t \in \mathbb{Z}[i]$.
   - Lastly, $N(t) = \frac{r_R^2 + r_I^2}{c^2 + d^2} \leq \frac{(c^2+d^2)^2 + (c^2+d^2)^2}{4(c^2+d^2)} \leq \frac{1}{2}(c^2 + d^2) < c^2 + d^2$.
3. - We could do it with numbers but it is a pain, let's do it geometrically. Let $e_1 = a + b\zeta_3$ and $e_2 = c + d\zeta_3$.
   - The lattice $L = e_1 + e_2\mathbb{Z}[\zeta_3]$ is mesh of equilateral triangles centered at e_1 and with sidelengths $N(e_2)$ and rotated $\text{Arg}(e_2)$ degrees. We would like to proof that there is a point of this grid in the closed ball centered at the origin and with radius $N(e_2)$.
   - Indeed, the largest ball that fits without having any lattice points is the circumscribed circle of the fundamental mesh, which has radius $\frac{\sqrt{3}}{3}N(e_2) < N(e_2)$. Hence, the origin ball must contain some point on the lattice.

Problem 3.3. [4, Ch.1, §2, p.5, Ex.3] *Show that the integers solutions of the equation*

$$x^2 + y^2 = z^2$$

such that $x, y, z > 0$ and $(x, y, z) = 1$ ("pythagorean triples") are all given, up to possible permutation of x, y by the formula

$$x = u^2 - v^2,\ y = 2uv,\ z = u^2 + v^2$$

where $u, v \in \mathbb{Z}$, $u, v > 0$, $(u, v) = 1$ and u, v not both odd.
***Hint**. Use Ex.2 above to show that $x + iy = \epsilon\alpha^2$, where $\alpha = u + iv \in \mathbb{Z}[i]$*

Solution.

- Let's first check that $x+iy$ and $x-iy$ are coprime in $\mathbb{Z}[i]$. Suppose not, then there would be a non-trivial common divisor $s + it$. Hence $s + it|x + iy$ and $s + it|x - iy$. Let $d = s^2 + t^2$.
  - We can take norms and get $d|x^2 + y^2 = z^2$.
  - Adding both congruences, $s + it|2x$ and $s + it|2y$, hence, taking norms $d|4x^2$ and $d|4y^2$.
  - d is a common divisor of $4x^2, 4y^2, z^2$ so, up to sign, it must be either 2 or 4. Recall $d = 1$ implies $s + it$ unit, which is not a non-trivial divisor.
  - Hence, $2|z^2 \implies 4|z^2$ so x and y must be odd and $x^2 + y^2 = 0 \mod 4$. But, the sum of two odd squares can only be congruent to 2, not 0.
  - Hence $x + iy$ and $x - iy$ are coprime on $\mathbb{Z}[i]$.
- $x^2 + y^2 = z^2 \implies (x + iy)(x - iy) = z^2$. Knowing $x + iy$ and $x - iy$ are relatively prime, by Problem 2, we have $x + iy = \epsilon(u + iv)^2$ with ϵ a unit. Then, $x = \epsilon(u^2 - v^2)$ and $y = \epsilon 2uv$.
- Recall units in $Z[i]$ are $1, -1, i, -i$ and $x, y \in \mathbb{Z}^+,\ u, v \in \mathbb{Z}$ implies $\epsilon = 1$, which finishes the proof.

HW4. September 26th

Problem 4.1. [2, p.30, Ex. 19] *Let R be a commutative ring and fix elements $a_1, a_2, \cdots \in R$. We will prove by induction that the Vandermonde determinant*

$$\begin{vmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{vmatrix}$$

is equal to the product $\prod_{1 \le r < s \le n}(a_s - a_r)$. Assuming that the result holds for some n, consider the determinant

$$\begin{vmatrix} 1 & a_1 & \cdots & a_1^{n} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n} \\ 1 & a_{n+1} & \cdots & a_{n+1}^{n} \end{vmatrix}$$

.
Show that this is equal to

$$\begin{vmatrix} 1 & a_1 & \cdots & f(a_1) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & f(a_n) \\ 1 & a_{n+1} & \cdots & f(a_{n+1}) \end{vmatrix}$$

.
for any monic polynomial f over R of degree n. Then choose f cleverly so that the determinant is easily calculated.

Solution.

- The determinant is invariant by adding to a column a linear combination of other columns. Since the other columns are precisely the powers of a_i, you can build any monic polynomial of degree n on a_i in this way.
- Choose $f(x) = (x - a_1) \cdots (x - a_n)$, evaluating at a_i the last column is all 0 but the last element which gives $(a_{n+1} - a_1) \cdots (a_{n+1} - a_n)$.
- Expanding the determinant by that row and applying the inductive step, we get the desired result.

Problem 4.2. *Using problem 4.1, show that if $K = \mathbb{Q}(\alpha)$ is a number field generated by an algebraic integer α, and f is the monic irreducible polynomial of α over $\mathbb{Q}$, then the discriminant of $\mathbb{Z}[\alpha]$ is equal, up to sign to $N_{K/\mathbb{Q}}(f'(\alpha))$.*

Solution.

- Let $f = a_0 + a_1 x + \cdots a_{n-1} x^{n-1} + x^n$, $a_i \in \mathbb{Z}$ be the minimal polynomial of α.
- Choose the base $\{1, \alpha, \cdots, \alpha^{n-1}\}$ of $\mathbb{Z}[\alpha]$.
- $\mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Z}$, so it is Galois. Hence we can use the discrminant formula in the Galois case.

$$\mathrm{Disc}(\mathbb{Z}[\alpha]) = \left(\mathrm{Det} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix} \right)^2 = \prod_{i \neq j} (\alpha_i - \alpha_j)^2 = f'(\alpha_1) \cdots f'(\alpha_n) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(f'(\alpha))$$

Problem 4.3. [2, Ch.2, Ex. 23] *Just as with the trace and norm, we can define the relative discriminant Disc_K^L of an n-tuple, for any pair of number fields $K \subseteq L$, $[L : K] = n$*

1. *Generalize Theorems 6-8 and the corollary to Theorem 6. [2, Ch.2]*
2. *Let $K \subseteq L \subseteq M$ be number fields, $[L : K] = n, [M : L] = m$ and let $\{\alpha_1, \cdots \alpha_n\}$ and $\{\beta_1, \cdots \beta_m\}$ be bases for L over K and M over L, respectively.*

   Establish the formula

   $$\mathrm{Disc}_K^M(\alpha_1\beta_1, \cdots, \alpha_n\beta_m) = (\mathrm{Disc}_K^L(\alpha_1, \cdots, \alpha_n))^m \cdot N_K^L(\mathrm{Disc}_L^M(\beta_1, \cdots, \beta_m))$$

   Hint. *There is a long suggestion in the book.*
3. *Let K and L be number fields satisfying the conditions of Corollary 1, Theorem 12. Show that* $(\mathrm{Disc}T) = (\mathrm{Disc}R)^{[L:\mathbb{Q}]}(\mathrm{Disc}S)^{[K:\mathbb{Q}]}$

Solution.

1. I state the new theorems in the relative case. As all the theorems deal with computing discriminants of a given tuple, the result will be integers, not ideals. The proofs are exactly the same as in the original setting. The setting is the following. L/K an extension of number fields, $\alpha_1, \ldots, \alpha_n \in L$
   - **Theorem 6.** $\mathrm{Disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{Det}(\mathrm{Tr}_K(\alpha_i\alpha_j))$, where $\mathrm{Tr}_K : L \to K$ is the generalized trace.
   - **Corollary.** $\mathrm{Disc}(\alpha_1, \ldots, \alpha_n) \in K$ and if all are algebraic integers, $\mathrm{Disc}(\alpha_1, \ldots, \alpha_n) \in \mathcal{O}_K$
   - **Theorem 8.** If $L = K[\alpha]$, with monic minimal polynomial $f \in K[x]$, and α_i all the roots of f, then

     $$\mathrm{Disc}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{i<j} (\alpha_i - \alpha_j) = \pm N_K(f'(\alpha))$$

     with $+$ iff $n = 0, 1 \mod 4$ and where $N_K : L \to K$ is the generalized norm.
2. - Let $\sigma_1, \ldots \sigma_n \in \mathrm{Aut}(L/K) \hookrightarrow \mathrm{Aut}(M/K)$ and $\tau_1, \ldots, t_n \in \mathrm{Aut}(M/L)$. By Galois theory, the $\sigma_i\tau_j \in \mathrm{Aut}(M/K)$ are all the automorphisms.

- Now,

$$\mathrm{Disc}_{L/K}(\alpha_i\beta_j) = \mathrm{Det}^2 \begin{pmatrix} \sigma_1\tau_1(\alpha_1\beta_1) & \sigma_1\tau_1(\alpha_2\beta_1) & \dots & \sigma_1\tau_1(\alpha_n\beta_m) \\ \sigma_2\tau_1(\alpha_1\beta_1) & \sigma_1\tau_2(\alpha_2\beta_1) & \dots & \sigma_1\tau_2(\alpha_n\beta_m) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n\tau_m(\alpha_1\beta_1) & \sigma_n\tau_m(\alpha_2\beta_1) & \dots & \sigma_n\tau_m(\alpha_n\beta_m) \end{pmatrix} =$$

$$= \mathrm{Det}^2 \begin{pmatrix} \sigma_1(\alpha_1)\sigma_1\tau_1(\beta_1) & \dots & \sigma_1(\alpha_n)\sigma_1\tau_1(\beta_m) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1)\sigma_n\tau_m(\beta_1) & \dots & \sigma_n(\alpha_n)\sigma_n\tau_m(\beta_m) \end{pmatrix} =$$

$$= \mathrm{Det}^2 \begin{pmatrix} S_1 & 0 & \dots & 0 \\ 0 & S_2 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & S_n \end{pmatrix} \mathrm{Det}^2 \begin{pmatrix} A_{11} & \dots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \dots & A_{nn} \end{pmatrix}$$

  , where $A_{ij} = \sigma_i(\alpha_j) \times \mathrm{Id}_m$ and

$$S_h = \sigma_h \begin{pmatrix} \tau_1(\beta_1) & \dots & \tau_1(\beta_m) \\ \vdots & \ddots & \vdots \\ \tau_m(\beta_1) & \ddots & \tau_m(\beta_m) \end{pmatrix}$$

  with σ_h applied element-wise.
- Computing the determinants as the product of blocks, we get the desired equality.

3. - If you have integral basis $\alpha_1 \dots \alpha_n$ of R and $\beta_1 \dots \beta_m$ of R, $\alpha_1\beta_1 \dots \alpha_n\beta_m$ is an integral basis of $T = \mathcal{O}_{R \cdot S}$.
   - By the proposition above applied to the chain $\mathbb{Z} \subseteq R \subseteq T$

$$\mathrm{Disc}T = (\mathrm{Disc}R)^m \cdot N_{R/\mathbb{Z}}(\mathrm{Disc}_{T/R}(\beta_1 \dots \beta_m)) = (\mathrm{Disc}R)^m(\mathrm{Disc}S)^n$$

   - In the last step, we are using that $\mathrm{Disc}_{T/R}(\beta_1, \dots, \beta_m) = \mathrm{Disc}_{S/\mathbb{Z}}(\beta_1, \dots, \beta_m)$. This is because the Galois groups $\mathrm{Aut}(S/\mathbb{Z}) = \mathrm{Aut}(T/R)$ and $\beta_1, \dots, \beta_m$ is a base of both extensions. Hence the computation of the determinant is exactly the same and gives the same result.
   - We are also using that the norm is just the n-th power if the elements is in the base field.

Problem 4.4. [2, Ch.2, Ex. 34] *Let $w = e^{2\pi i/m}$, m a positive integer.*

1. *Show that $1 + w + w^2 + \cdots + w^{k-1}$ is a unit in $\mathbb{Z}[w]$ if k is relatively prime to m.*
   ***Hint:** Its inverse is $(w-1)/(w^k-1)$; show that $w = w^{hk}$ for some $h \in \mathbb{Z}$.*
2. *Let $m = p^r$, p a prime. Show that $p = u(1-w)^n$ where $n = \phi(p^r)$ and u is a unit in $\mathbb{Z}[w]$.*
   ***Hint.** See Lemma 2, Theorem 2 [2, Ch.2]*

Solution.

1. - Following the hint, we only need to show that if $(k, m) = 1$, $w = w^{hk}$ for some $h \in \mathbb{Z}$. If this is shown, then the inverse of $1 + \cdots + w^{k-1}$ will be $1 + w^k \cdots + w^{k(h-1)}$, which is clearly in $\mathbb{Z}[w]$.
   - Let $\lambda(m)$ be the group of m-th roots of unity with the usual complex product. It is a cyclic group of order m generated by w. If $(k, m) = 1$, the automorphism $x \mapsto x^k$ is injective as $x \neq 1$ and $x^k = 1 \implies (x)$ is a non-trivial subgroup of order $d|k$ but $d \not| m$ by coprimality.
   - An injective morphism on a finite group is surjective so there is some element w^h that maps onto w, giving $w = w^{hk}$.

2. - Lemma 2 in [2] gives the following identity. If $w = e^{\frac{2\pi i}{p^r}}$, we have

$$\prod_{1 \leq k \leq p^r \text{ st } p \not| k} (1 - w^k) = p$$

   - We can multiply both sides by $\frac{w-1}{/}1 - w^k$, which are units of $\mathbb{Z}[w]$ for all k coprime with p^r, or equivallently $p \not| k$. Note that there are $\phi(p^r)$ such k. We get the desired result

$$(w-1)^{\phi(p^r)} = p \cdot (\text{unit})$$

HW5. October 3rd

Problem 5.1. *Give and example of two different number field K_1 and K_2 such that there is a prime p which is totally ramified in both K_1 and K_2 but not totally ramified in the compositum $K_1 \cdot K_2$.*

Solution.

- Choose $K_1 = \mathbb{Q}(\sqrt{3})$ and $K_2 = \mathbb{Q}(\sqrt{7})$, quadratic fields. From problems 1.1 and 3.1 we know that the rings of integers are $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Z}[\sqrt{7}]$ respectively and the discriminants are $4 \cdot 3$ and $4 \cdot 7$ respectively.
- In both cases 2|Disc, so 2 ramified.
- Because they are extension of degree 2, ramified implies completely ramified.
- Their compositum $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ which contains $\mathbb{Q}(\sqrt{21})$ as a subfield. But $21 \equiv 1 \mod 4$, so the discriminant is 21 (odd), so 2 splits $(2) = \mathfrak{p}_1\mathfrak{p}_2$.
- As 2 splits in a subfield, the only way for it to completely ramify in the higher field is if $\mathfrak{p}_1\mathcal{O} = \mathfrak{p}_2\mathcal{O}$ but that would imply $\mathfrak{p}_1 = \mathfrak{p}_2$, which is a contradiction. Hence 2 is not completely ramified in the compositum.

Problem 5.2. *Let $N > 0$ be an integer and consider the ring*

$$\mathbb{Z}_N = \varprojlim_n \mathbb{Z}/N^n\mathbb{Z}$$

Show that there is a natural isomorphism

$$\mathbb{Z}_N \simeq \prod_{p|N} \mathbb{Z}_p$$

where the right product is taken over primes dividing N.

Solution.

- By Chinese Remainder Theorem, $\mathbb{Z}/N^n\mathbb{Z} = \prod \mathbb{Z}/p_i^{e_i n}\mathbb{Z}$ and the inverse limit distributes with the product.
- For a fixed constant e, $\varprojlim_n \mathbb{Z}/p^{en}\mathbb{Z} = \mathbb{Z}_p$ as finite jumps don't matter as long as you have p^{k_n} arbitrarily large, the other values are completely determined by the inverse system.

Problem 5.3. *Let A be a complete discrete valuation ring whose fraction field is of characteristic 0 and whose residue field k is perfect of characteristic $p > 0$. Show that for every $x \in k$ there exists a unique lifting of x to A with has a p^n-th root in A for all positive integers n. This lifting is usually denoted $[x]$.*

Solution.

- Let π be a uniformizer of the d.v.r and $A = \varprojlim_m A/\pi^m$
- We have a value $x \in A/\pi$ which is a p^n-th power for all n, by A/π perfect.
- We will show that there is a unique lift of x in each A/π^m that is a perfect p^n-th power for all n by induction on m. Compatible elements of the inverse system will give the desired element of the inverse limit.
- Suppose $r_m \in A/\pi^m$ is the unique lift of x that is a perfect p^n-power for all n.
- Any lift will be of the form $r_{m+1} = r_m + \beta\pi^m$, with $\beta \in A/\pi$
- For any n, we need consider the polynomial $T^{p^n} - r_m - \beta\pi^m$. We need to choose β such that all these polynomials have roots in A/π^{n+1}
- By the induction hypothesis, looking $\mod \pi^m$, $T^{p^n} - r_m$ has a solution $u_n \in A/\pi^m$
- A lift of this solution will have the form $u_n + \gamma_n\pi^n$, with $\gamma_n \in A/\pi$. We get

$$(u_n + \gamma_n\pi^n)^{p^n} - r_m - \beta\pi^n = u_n^{p^n} - r_m + p^n u_n^{p^n-1}\pi^n\gamma_n - \beta\pi^n$$

- All of the other terms in the power get canceled $\mod \pi^{n+1}$ as they have a factor $\pi^{kn}, k > 1$.
- By induction, we know $\pi^n \mid u_n^{p^n} - r_m \implies u_n^{p^n} - r_m = s_n \pi^n$

$$u_n^{p^n} - r_m + p^n u_n^{p^n-1} \pi^n \gamma_n - \beta \pi^n = \pi^n s_n + p^n u_n^{p^n-1} \pi^n \gamma_n - \beta \pi^n = \pi^n (s_n + p^n u_n^{p^n-1} \gamma_n - \beta)$$

- For this to be $0 \mod \pi^{n+1}$, the part inside of the parenthesis must be divisible by π
- Going to A/m, we need $\beta = s_n + p^n u_n^{p^n-1} \gamma_n = s_n \mod \pi$.

TODO. I need to see the s_n don't depend on n

Problem 5.4. [5, Ex.1, p.30, (Krasner's lemma)] *Let E/K be a finite Galois extension of a complete field K. Prolong the valuation of K to E. Let $x \in E$ and let $\{x_1, \cdots, x_n\}$ be the set of conjugates of x over K, with $x = x_1$. Let $y \in E$ be such that $||y - x|| < ||y - x_i||$ for $i \geq 2$. Show that x belongs to the field $K(y)$.*
Hint. *Note that if x_i is conjugate of x over $K(y)$, then $||y - x|| = ||y - x_i||$.*

Solution.

- Suppose that there is a $\sigma \in \mathrm{Aut}(E/K)$ that moved $\sigma(x) = x_i$ but made was fixed on $K(y)$. Then $||y - x|| = ||\sigma(y) - \sigma(x)|| = ||y - x_i||$, contradicting the statement.
- In the first equality we are using completeness of K to state that the norms $||\cdot||$ and $||\cdot|| \circ \sigma$ are both extension of the norm in K and hence equivalent. Looking at both in K we can fix the equivalence constant to 1.
- Hence for all $\sigma \in \mathrm{Aut}(E/K(y))$, $\sigma(x) = x$, which, by the Galois correspondence, implies $x \in K(y)$.

HW6. October 17th

Problem 6.1. [5, Ex. 1, 2, 3, p.59]

1. *In the AKBL setting. Suppose that B (hence also A) is a DVR and suppose the extension l/k of residue fields is separable. Show that if $B = A[x]$, and y is sufficiently near to x, then $B = A[y]$.*

   Hint. *With these hypothesis, Prop. 12 [5] proves that B has a power basis on A.*

2. *In the general case, let $\mathfrak{B}$ be a prime ideal of B whose corresponding residue extension is separable. Show that there exists an $x \in B$ generating the extension L/K such that the conductor r of B in $A[x]$ is prime to $\mathfrak{B}$*

   Hint. *Apply problem 1 to the completions of B and A.*

3. *Suppose that A is a discrete valuation ring and that B is "completely decomposed", i.e., that there are $n = [L : K]$ prime ideals of B above the prime ideal p of A. Show that in order for there to exist an $x \in B$ such that $B = A[x]$, it is necessary and sufficient that $n \leq Card(\overline{K})$, where $\overline{K}$ is the residue field of A.*

Solution. TODO

Problem 6.2. [4, Ex. 3, p.176] *Show that the maximal unramified extension of the power series field $K = \mathbb{F}_p((t))$ is given by $T = \overline{\mathbb{F}_p}((t))$ where $\overline{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_p$ and the maximal tamely ramified extension by $T(\{\sqrt[m]{t} \mid m \in \mathbb{Z}, (m, p) = 1\})$.*

Solution.
TODO

Problem 6.3. [4, Ex. 1, 2, 3, p.142]

1. *The logarithm function can be continued to a continuous homomorphism $\log : \overline{\mathbb{Q}_p^*} \to \mathbb{Q}$ and the exponential to a continuous homomorphism $\exp : \overline{\mathfrak{p}}^{\frac{1}{1-p}} \to \overline{\mathbb{Q}_p^*}$, where $\overline{\mathfrak{p}}^{\frac{1}{1-p}} = \{x \in \overline{\mathbb{Q}_p} \mid \nu_p(x) > \frac{1}{1-p}\}$ and ν_p is the unique extensions of the normalized valulation on $\mathbb{Q}_p$*

2. *Let $K/\mathbb{Q}_p$ be a $\mathfrak{p}$-adic number field. For $1+x \in U^{(l)}$ and $z \in \mathbb{Z}_p$, one has*

$$(1+x)^z = \sum_{v=0}^{\infty} \binom{z}{v} x^v$$

The series converges even for $x \in K$ such that $\nu_p(x) > \frac{e}{p-1}$

3. *Under the above hypotheses one has*

$$(1+x)^z = \exp(z\log(1+x)) \quad \text{and} \quad \log(1+x)^z = z\log(1+x)$$

Solution. TODO

HW7. October 24th

Problem 7.1. *Please write a few sentences suggesting a topic for your term paper.*

I would be interested in writing about Artin's primitive root conjecture, in particular about the proof of the conjecture in the function field setting, due to Herbert Bilharz and depending on the Weil Conjectures. This corresponds to Chapter 10 in M.Rosen *Number Theory in Function Fields.*

This topic fits my interests because I am currently working with Prof. Shin towards proving a generalization of Artin's conjecture with a different, more elementary, strategy given by a recent paper by Seoyoung Kim and M. Ram Murty.

Problem 7.2. [3, Ex. 4-4, 4–7]

1. *Show that $\mathbb{Q}(\sqrt{-23})$ has class number 3 and that $\mathbb{Q}(\sqrt{-47})$ has class number 5.*

2. *Let $\mathbb{Q}[\sqrt{-1},\sqrt{5}]$. Show that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}, \frac{1+\sqrt{5}}{2}]$. Show that the only primes (in $\mathbb{Z}$) that ramify in K are 2 and 5, and that their ramification indexes are both 2. Deduce that K is unramified over $\mathbb{Q}[\sqrt{-5}]$. Prove that $\mathbb{Q}[\sqrt{-5}]$ has class number 2, and deduce that K is the Hilbert class field of $\mathbb{Q}[\sqrt{-5}]$*

Solution.

1.

- Note that, for D square-free, $\mathbb{Q}(\sqrt{D})$ is Galois over $\mathbb{Q}$.
- $\boxed{\mathbb{Q}[\sqrt{-23}]}$
  - The constants in the Minkowski bound are $r_1 = 0, r_2 = 1, d = 2$. By Problem 3.1 Disc $= -23$, which gives $B = \frac{2!}{2^2}(\frac{4}{\pi})^1\sqrt{23} \approx 3.05$
  - If $J = \beta_1^{\alpha_1}\dots\beta_g^{\alpha_g}$, $N(J) = p_1^{\alpha_1 f_1}\cdots p_g^{\alpha_g f_g}$. Where $p_i = \beta_i \cap \mathbb{Z}$. For this to be ≤ 3, we need $\mathfrak{p}_i \in 2, 3$ and $\alpha_i f_i = 1$.
  - Hence, Minkoski bound states that every element of the class group has a representative as some J that can be either prime over 2 or 3.
  - Note that 2, 3 don't divide the discriminant, so they don't ramify. They either split into two primes or stay inert.
  - $\frac{1}{2}(1+\sqrt{-23})\times\frac{1}{2}(1-\sqrt{-23}) = 6 \in (2)$, and neither of the terms are in $(2) = \{a+\frac{b}{2}(1+\sqrt{D}) \mid a, b \in \mathbb{Z} \text{ even}\}$. Hence (2) is not a prime ideal in $\mathcal{O}$, so it splits $(2) = \mathfrak{p}_1\mathfrak{p}_2$.
  - We found $\frac{1}{2}(1+\sqrt{-23}) \mid (2)$ but is not in (2), so $\mathfrak{p}_1 = (2, \frac{1}{2}(1+\sqrt{-23})) \mid (2)$ but is not (2). As we are in the Galois case, $\mathfrak{p}_2 = \overline{\mathfrak{p}_1}$
  - Exactly as before, $\frac{1}{2}(1+\sqrt{-23}) \times \frac{1}{2}(1-\sqrt{-23}) = 6 \in (3)$ but neither of the terms is in $(3) = \{a+\frac{b}{2}(1+\sqrt{D}) \mid a, b \in \mathbb{Z}, a \equiv b \equiv 0 \mod 3\}$. Hence (3) is not prime, it splits as the product of two distinct primes $(3) = \mathfrak{p}_3\mathfrak{p}_4$.
  - By the same reasons as (2), $\mathfrak{p}_3 = (3, \frac{1}{2}(1+\sqrt{-23})$ and $\mathfrak{p}_4 = \overline{\mathfrak{p}_3}$.

– But,

$$\mathfrak{p}_1\mathfrak{p}_3^{-1} = \mathfrak{p}_1\mathfrak{p}_4 = \left(6, 1-\sqrt{-23}, \frac{3}{2}(1+\sqrt{-23}), \frac{1}{4}(1+23)\right) = \left(\frac{1}{2}(1+\sqrt{-23})\right)$$

so, $\mathfrak{p}_1 \sim \mathfrak{p}_3$ in the class group.

– Hence, the class group has 3 elements, $\{1, \mathfrak{p}_1 = \mathfrak{p}_3, \mathfrak{p}_2 = \mathfrak{p}_4\}$.

- $\boxed{\mathbb{Q}[\sqrt{-47}]}$
  – The constants in the Minkowski bound are $r_1 = 0, r_2 = 1, d = 2$. By Problem 3.1 Disc $= -47$, which gives $B = \frac{2!}{2^2}(\frac{4}{\pi})^1\sqrt{47} \approx 4.36$
  – If $N(J) \leq 4$, J can again only have factors above 2 and 3. Again, neither of them ramify as they don't divide the discriminant, either they decompose as a product of 2 prime ideals, or they are inert.

  – We also count with the fact that $\frac{1}{2}(1+\sqrt{-47})\frac{1}{2}(1-\sqrt{-47}) = 12 \in (2)$ and $\in (3)$ but neither of the factors are in (2) nor in (3).
  – By the same reasons as in $D = -23$ case, $(2) = \mathfrak{p}_1\mathfrak{p}_2$ and $(3) = \mathfrak{p}_3\mathfrak{p}_4$, with $\mathfrak{p}_1 = (2, \frac{1}{2}(1+\sqrt{-47}))$ and $\mathfrak{p}_3 = (3, \frac{1}{2}(1+\sqrt{-47}))$

  – This time,

$$\mathfrak{p}_1\mathfrak{p}_3^{-1} = \left(6, 1-\sqrt{-47}, \frac{3}{2}(1+\sqrt{-47}, \frac{1}{4}(1+47))\right) = \left(1-\sqrt{-47}, \frac{3}{2}(1+\sqrt{-47}\right)$$

as $6 = 2\left(\frac{3}{2}(1+\sqrt{-47})\right) + 3\left(1-\sqrt{-47}\right)$. This ideal is not principal as $N\left(1-\sqrt{-47}\right) = 48$, $N\left(\frac{3}{2}(1+\sqrt{-47})\right) = 108$ and $48 \not| 108$.
  – Hence, the class group is $\{1, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4\}$, with order five.

2. - Note $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-5})$, $\mathcal{O} = \mathcal{O}_K$. We will also note $i = \sqrt{-1}$, $\phi = \frac{1+\sqrt{5}}{2}$ and $\widehat{\phi} = \frac{1-\sqrt{5}}{2}$.
   - We will use that $\mathbb{Q}(i), \mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-5})$ are all subextensions of $K/\mathbb{Q}$. For a prime in p to ramify completely over K, it need at least to ramify over each of the subextensions.

   - $\mathbb{Z}[i, \phi] \subseteq \mathcal{O}$ from the monic integer polynomials x^2+1 and x^2-x-1. Also, note $\sqrt{5} = i\sqrt{-5}$, hence it is in K.
   - Let's compute the discriminant of $\mathbb{Z}[i, \phi]$ over $Z[i]$. Take $\{1, \phi\}$ as a basis. Using the formula of the discriminant in the Galois case, we get

$$\text{Disc}_{\mathbb{Z}[i,\phi]} = \text{Det}^2\begin{pmatrix} 1 & \phi \\ 1 & \widehat{\phi} \end{pmatrix} = 5$$

whose Gaussian prime decomposition is $(1+2i)(1-2i)$, hence it is not a square in $\mathbb{Z}[i]$. Hence $\mathcal{O} = \mathbb{Z}[i, \phi]$.
   - In problem 2.2, we saw that 2 and 5 ramify on $\mathbb{Q}(\sqrt{-5}) \subseteq K$ so they must ramify in K. Nonetheless, $2, 5$ do not ramify in $\mathbb{Z}[i]$, so they can not totally ramify in K.

   - The Minkoski bound on $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Q} = \frac{2}{2^2}(\frac{4}{\pi})\sqrt{20} = 2.8$, hence any non principal ideal must be over 2. The only ideal over 2 is $(2, 1+\sqrt{-5})$ which, as we proved in Problem 2.2, is not principal. Hence the class group is $\mathbb{Z}/2\mathbb{Z}$.
   - Note that $K/\mathbb{Q}(\sqrt{-5})$ is Galois of degree 2 and with Galois group $\{1, \sigma\}$, with σ the complex conjugation.
   - As the only primes ramified over $\mathbb{Z}$ are 2 and 5 with ramification 2 and those already ramified over $\mathbb{Q}(\sqrt{-5})$, the extension $\mathbb{Q}(\sqrt{-5}) \hookrightarrow K$ is unramified. By being unramified and having Galois group isomorphic to the class group of $\mathbb{Q}(\sqrt{-5})$, K is the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$

Problem 7.3. [4, Ex. 2, p. 38] *Show that the quadratic fields with discriminant 5, 8, 11, -3, -4, -7, -8, -11 have class number 1.*

D	5	2	11	-3	-1	-7	-2	-11
Disc	5	8	11	-3	-4	-7	-8	-11
r_1	2	2	2	0	0	0	0	0
r_2	0	0	0	1	1	1	1	1
$B_K \approx$	1.11	1.41	1.65	1.10	1.27	1.68	1.80	2.11

Solution.

- The Minkowski bounds are
- In all of them but the last, for any I in the class group, there is a representative J with $N(J) = 1$. This implies $J = \mathcal{O}$, which is principal generated by any unit. Hence, the class group is trivial.
- The case of -11 has to be done separately as the representative J could be a prime over 2. $2 \nmid -11$, so it doesn't ramify so it's either inert or split in two.
- Suppose

$$\left(a + \frac{b}{2}(1 + \sqrt{-11})\right)\left(c + \frac{d}{2}(1 + \sqrt{-11})\right) \in (2) \iff$$
$$ac - 3bd = cb + ad + bd = 0 \mod 2$$

  which only has solutions with either $a = b = 0$ or $c = d = 0$, proving (2) is a prime in $\mathcal{O}$.
- Hence, the class group is trivial.

HW8. November 7th

Problem 8.1. *Let D be a positive integer not congruent to* $1 \mod 4$

1. *Show that if $a^2 - Db^2 = 1$ and $a + b\sqrt{D} > 1$ (in the sense of real numbers) then $a > 1$ and $b > 0$*
   Hint. *Notice that $(a + b\sqrt{D})^{-1} = a - b\sqrt{D}$ and therefore we have $a + b\sqrt{D} > 1 > a - b\sqrt{D} > 0$.*
2. *Let K be the field $\mathbb{Q}(\sqrt{D})$ and let U be the unit group of $\mathcal{O}_K$. Show that there exists a fundamental unit $u \in U$ of the form $a + b\sqrt{D}$ with a and b positive, by showing that if a unit $u = a + b\sqrt{D}$ satisfies the two conditions*
   (a) a and b are positive
   (b) $a + b\sqrt{D} > 1$

   and b is minimal subject to these conditions, then u is a fundamental unit

Solution.

1. - $a + b\sqrt{D} > 1$ and $1 > a - b\sqrt{D} > 0$ imply $2b\sqrt{D} > 0 \implies b > 0$ and, similarly, $a > 1/2$.
   - Since $a^2 = 1 + Db^2 > 1$ and $a > 1/2 > 0$ we have $a > 1$.
2. - Units excluding ± 1 come in pairs, $|a + b\sqrt{D}| > 1 \iff |a - b\sqrt{D}| < 1$. Hence to look for a fundamental unit, we may restrict to only the first case.
   - $|a + b\sqrt{D}| > 1$ is a unit, then a and b must have the same sign as $|a - b\sqrt{D}| < 1$. As ± 1 are roots of unity, we can restrict the search to $a, b > 0$.
   - For $a + b\sqrt{D} > 1$, $a, b > 0$ to be a fundamental unit, it must be the (a, b) that minimizes the value $a + b\sqrt{D}$. If there was a tuple with smaller value but still > 1, $(a + b\sqrt{D})^n$ would never reach that value. This necessary condition is also enough by the Unit Theorem.
   - Minimizing only over b is enough as $a = \sqrt{\pm 1 + Db^2}$ which, in both cases, is monotone with respect to b. This is to say that the tuple minimizing b will also minimize $a + b\sqrt{D}$.

Problem 8.2. [4, Ex. 1, p.43] *Let $D > 1$ be a squarefree integer and d the discriminant of the real quadratic number field $K = \mathbb{Q}(\sqrt{D})$. Let x_1, y_1 be the uniquely determined rational integer solution of the equation*

$$x^2 - dy^2 = -4$$

or, in case this equation has no rational integer solutions, of the equation

$$x^2 - dy^2 = 4$$

for which $x_1, y_1 > 0$ are as small as possible. Then

$$\varepsilon_1 = \frac{x_1 + y_1\sqrt{d}}{2}$$

is a fundamental unit of K.

- In the real quadratic case, units come in pairs, one with absolute value > 1 and, its conjugate with < 1, as their product is ± 1 and the only units with absolute value 1 are ± 1.
- Hence, one will be able to find a fundamental unit with > 1. This will necessarily be the one that that minimizes absolute value, as $|a| > 1 \implies |a|^k > |a|$ for $k > 1$.
- $\boxed{D \equiv 1 \mod 4}$
  - $d = D$ and $\{1, \frac{1+\sqrt{D}}{2}\}$ is an integral basis
  - $u = \frac{x+y\sqrt{D}}{2}$ is a unit $\iff N(u) = \frac{x^2 - Dy^2}{4} = \pm 1 \iff x^2 - Dy^2 = \pm 4$
- $\boxed{D \not\equiv 1 \mod 4}$
  - $d = 4D$ and $\{1, \sqrt{D}\}$ is an integral basis
  - If $x^2 - 4Dy^2 = \pm 4 \implies x$ is even.
  - Now, $u = \frac{x}{2} + \frac{y}{2}\sqrt{4D}$ is a unit $\iff \frac{x^2}{4} - 4D\frac{y^2}{4} = \pm 1 \iff x^2 - 4Dy^2 = \pm 4$.
- In both cases taking (x, y) that minimize the absolute value of u corresponds to taking x, y solution of the equations in the priority stated. Per the observation, that proves that choice of x, y gives a fundamental unit.

References

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. 1969.

[2] Daniel A. Marcus. *Number fields*. 2018.

[3] James S. Milne. *Algebraic number theory*. 2020.

[4] Jürgen Neukirch. *Algebraic number theory*. 1992.

[5] Jean-Pierre Serre. *Local fields*. 1979.