F i n a l   E x a m i n a t i o n

Stephanie N. Reyes

Submitted to Instructor: December 16, 2019 11:00AM(CST)

By signing above, the author affirms her adherence to the official policy on Academic Integrity, set forth by the University of Illinois at Chicago, in completing the enclosed response to the final examination, written and distributed by the instructor Dr. Alina Carmen Cojocaru, for the **Fall 2019** iteration of **Math 514**: Number Theory I.

Chicago, Illinois

The instructor has specified the following allowances:

i. Students **may** collaborate in devising solutions;

ii. students **must** write solutions individually;

iii. students **may** consult references but **must** properly cite all technical references.

CONTENT WARNING(S): Citas filosófico de *Futurama*.

STYLE WARNING(S): The author rates this work **TV14—PG13.** This author **is not** a suitable role model for children or impressionable youngsters. She has a particular flair for making very complicated concepts *seem* elementary—her solutions are deceptively simple and algorithmic, but she takes care to weave deep intuition and understanding of mathematics into her calculations. Her *pseudo*-academic voice is an intentional allusion to her working class background. This author's work is known to contain any one or more of the following items:

A. Academic snark. Opinionated remarks, cultural criticisms, boasts and humblebrags, cleverly-coined technical terms;

B. Working Class Enthusiasm. ¡Exclamations and exclamation points! harmless cursing, authentic joy, strange spanglish, cultural code switching, nonstandard notation, weird usage of words, excessive alliteration.

PRO-TIP—If you don't understand something strange, don't worry about it.

Exercise I.

Let K be a number field with $[K:\mathbb{Q}]=n$; let $0\neq I\trianglelefteq\mathcal{O}_K$ be a nonzero ideal; and let $e_1,\ldots,e_n,\ f_1,\ldots,f_n\in I$ be such that $\{e_1,\ldots,e_n\}$ is a $\mathbb{Z}$-basis for I and such that $\operatorname{disc}_{K/\mathbb{Q}}(e_1,\ldots,e_n)=\operatorname{disc}_{K/\mathbb{Q}}(f_1,\ldots,f_n)$.

Given a matrix $A=(a_{ij})$, we will use the notation $A_i=(a_{ij})_i$ and $A^j=(a_{ij})^j$ to denote the i^{th} row vector and j^{th} column vectors of A, respectively. We will consider 1×1 matrices as scalars, so that given A and B, the $(i,\ j)$-th entry of their product AB is A_iB^j. Given a map σ of *scalars* we denote $\sigma(A)\ :=\ (\sigma(a_{ij}))$.
Note that if σ is a morphism of rings, then $\sigma(AB)\ =\ \sigma(A)\,\sigma(B)$.

Exercise I. Prove that $\{f_1,\ldots,f_n\}$ is also a $\mathbb{Z}$-basis for I.

Proof. Let $\sigma_i\ :\ K\hookrightarrow\mathbb{C}$ for $i=1,2,\ldots,n$ denote the n distinct embeddings of K into $\mathbb{C}$. Because $\{e_1,\ldots,e_n\}$ is a $\mathbb{Z}$-basis for I there exist $a_{ij}\in\mathbb{Z}$ for $i,j=1,2,\ldots,n$ such that $f_i=\sum_{j=1}^{n}a_{ij}e_j$. In other words, $A\ :=\ (a_{ij})$ is a matrix with integer entries, and $E\ :=\ (e_i)$ and $F\ :=\ (f_i)$ are column vectors such that $F=AE$ and $f_i=A_iE$ as products of matrices.
Define $\sigma(E)\ :=\ (\sigma_j(e_i))$ so that its j^{th} column is $\sigma(E)^j=\sigma_j(E)$; similarly define $\sigma(F)\ :=\ (\sigma_j(f_i))$. Recalling that each σ_j restricts to the identity on $\mathbb{Z}$, we have that $\sigma_j(A_i)=A_i$ for all $1\leqslant i,\ j\leqslant n$. Then

$$\sigma(F)\ =\ (\sigma_j(f_i))\ =\ (\sigma_j(A_iE))\ =\ (A_i\sigma_j(E))\ =\ (A_i\sigma(E)^j)\ =\ A\,\sigma(E),$$

so because determinant is invariant under transpose we have that

$$
\begin{aligned}
\mathrm{disc}_{K/\mathbb{Q}}\,(f_1\,,\ldots,\,f_n) \quad = \quad \det(\sigma_i(f_j))^2 \quad &= \quad \det(\sigma(F))^2 \\
&= \quad \det(A\;\sigma(E))^2 \\
&= \quad \det(A)^2\;\det(\sigma(E))^2 \\
&= \quad \det(A)^2\;\mathrm{disc}_{K/\mathbb{Q}}\,(e_1\,,\ldots,\,e_n).
\end{aligned}
$$

Because $\mathrm{disc}_{K/\mathbb{Q}}\,(e_1\,,\ldots,\,e_n) = \mathrm{disc}_{K/\mathbb{Q}}\,(f_1\,,\ldots,\,f_n)$, we have $\det(A)^2 = 1$. So, there exists an inverse matrix $A^{-1} := B = (b_{ij})$ with integer entries. In terms of B, we can write $e_i = \sum_{j=1}^{n} b_{ij} f_j$ and $E = BF$ so that, for any $\alpha = \sum_{i=1}^{n} c_i e_j = CE \in I$ given by a row vector $C = (c_1\; c_2\; \cdots\; c_n)$ with integer entries, we have that CB is also a row vector with integer entries and that $\alpha = C\,E = C\,(B\,F) = (C\,B)\,F$.

Thus $\{f_1\,,\ldots,\,f_n\}$ is also a $\mathbb{Z}$-basis for I. □

Exercise II.

Let K be a number field with $[K:\mathbb{Q}] = n$ and let $\varepsilon \in \mathcal{O}_K$ be such that $K = \mathbb{Q}(\varepsilon)$. Recall from the text [AW04, p. 146], that there exists a positive integer $\operatorname{ind} \varepsilon$ such that

$$\operatorname{disc}_{K/\mathbb{Q}}(1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}) = (\operatorname{ind} \varepsilon)^2 (\operatorname{disc} K/\mathbb{Q}). \qquad (*)$$

Exercise II.1. Prove that $\{1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}\}$ is an integral basis for K if and only if $\operatorname{ind} \varepsilon = 1$.

Proof. The set $\{1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}\} \subseteq \mathcal{O}_K$ is an integral basis for K if and only if $\operatorname{disc}_{K/\mathbb{Q}}(1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}) = \operatorname{disc} K$ by Theorem [AW04, 6.5.4]. This is true if and only if $\operatorname{disc}_{K/\mathbb{Q}} \varepsilon = \operatorname{disc} K$ which, in turn, is true if and only if $\operatorname{ind} \varepsilon = 1$. $\square$

Exercise II.2. If $f(X) := X^3 + aX + b \in \mathbb{Z}[X]$ is the minimal polynomial of $\varepsilon \in \mathcal{O}_K$, prove that

$$\operatorname{disc}_{K/\mathbb{Q}}(1, \varepsilon, \varepsilon^2) = -4a^3 - 27b^2.$$

Proof. Setting $\varepsilon_1 := \varepsilon$, define ε_2 and ε_3 to be the Galois conjugates of ε_1 so that $(x-\varepsilon_1)(x-\varepsilon_2)(x-\varepsilon_3) = X^3 + aX + b$. After expanding the lefthand side of the above equation, we see that

$$\begin{aligned} 0 &= \varepsilon_1 + \varepsilon_2 + \varepsilon_3, \\ a &= \varepsilon_1\varepsilon_2 + \varepsilon_2\varepsilon_3 + \varepsilon_1\varepsilon_3, \qquad \text{and} \\ -b &= \varepsilon_1\varepsilon_2\varepsilon_3. \end{aligned}$$

Now, since $f'(X) = 3X^2 + a$, we have that

$$\begin{aligned} f'(\varepsilon_1)\ f'(\varepsilon_2)\ f'(\varepsilon_3) &= (3\ \varepsilon_1^2 + a)\ (3\ \varepsilon_2^2 + a)\ (3\ \varepsilon_3^2 + a) \\ &= a^3 + 3\ a^2\ (\varepsilon_1^2 + \varepsilon_2^2 + \varepsilon_3^2) \\ &\quad + 9\ a\ (\varepsilon_1^2\ \varepsilon_3^2 + \varepsilon_2^2\ \varepsilon_3^2 + \varepsilon_3^2\ \varepsilon_1^2) + 27\ \varepsilon_1^2\ \varepsilon_2^2\ \varepsilon_3^2. \end{aligned}$$

Next, we observe that

$$\begin{aligned} \varepsilon_1^2 + \varepsilon_2^2 + \varepsilon_3^2 &= (\varepsilon_2 + \varepsilon_2 + \varepsilon_3)^2 - 2\ (\varepsilon_1\ \varepsilon_2 + \varepsilon_2\ \varepsilon_3 + \varepsilon_3\ \varepsilon_1) \\ &= -2\ a, \\ \varepsilon_1^2\ \varepsilon_2^2 + \varepsilon_2^2\ \varepsilon_3^2 + \varepsilon_1^2\ \varepsilon_3^2 &= (\varepsilon_1\ \varepsilon_2 + \varepsilon_2\ \varepsilon_3 + \varepsilon_1\ \varepsilon_3)^2 \\ &\quad - 2\ \varepsilon_1\ \varepsilon_2\ \varepsilon_3\ (\varepsilon_1 + \varepsilon_2 + \varepsilon_3) \\ &= a^2, \qquad \text{and} \\ \varepsilon_1^2\ \varepsilon_2^2\ \varepsilon_3^2 &= (\varepsilon_1\ \varepsilon_2\ \varepsilon_3)^2 \\ &= b^2 \end{aligned}$$

implying that

$$\begin{aligned} f'(\varepsilon_1)\ f'(\varepsilon_2)\ f'(\varepsilon_3) &= a^3 + (3\ a^2)(-2\ a) + (9a)\ (a^2) + 27\ b^2 \\ &= 4\ a^3 + 27\ b^2. \end{aligned}$$

This, together with Theorem [AW04, 7.1.9], further implies that

$$\begin{aligned} \operatorname{disc}_{K/\mathbb{Q}}\ \varepsilon &= (-1)^{\frac{(3)(2)}{2}}\ f'(\varepsilon_1)\ f'(\varepsilon_2)\ f'(\varepsilon_3) \\ &= -4\ a^3 - 27\ b^2, \end{aligned}$$

as desired. □

Let $\varepsilon \in \mathbb{C}$ be a root of the polynomial $f(X) := X^3 + X + 1$, and let $K := \mathbb{Q}(\varepsilon)$.

Exercise II. Prove that $\{1, \varepsilon, \varepsilon^2\}$ is an integral basis for K and that $\operatorname{disc} K/\mathbb{Q} = -31$.

Proof. By Exercise II.2, we compute

$$\begin{aligned} \operatorname{disc}_{K/\mathbb{Q}}(1, \varepsilon, \varepsilon^2) &= -4\, a^3 - 27\, b^2 \\ &= (-4)\,(1)^3 + -27\,(1)^2 \\ &= -4 - 27 \\ &= -31. \end{aligned}$$

Because -31 is squarefree, we conclude from $(*)$ that $\operatorname{ind} \varepsilon = 1$ and that $\operatorname{disc} K/\mathbb{Q} = -31$. Finally, because $\operatorname{ind} \varepsilon = 1$, we conclude that $\{1, \varepsilon, \varepsilon^2\}$ is an integral basis by Exercise II.1. □

Exercise III.

Let $K := \mathbb{Q}(\sqrt{6})$. Then, K is a square number field with $d = 6 \equiv 2 \pmod 4$, implying that $\mathcal{O}_K = \mathbb{Z}[\sqrt{6}]$. Recall that $\mathcal{O}_K$ is a dedekind domain and consider ideals $P,\ Q,\ I \lhd \mathcal{O}_K$,

$$\begin{aligned} P &:= (2,\ \sqrt{6}), \\ Q &:= (3,\ \sqrt{6}) \quad \text{and} \\ I &:= (\sqrt{6}). \end{aligned}$$

Observation 1. $P = 2\,\mathbb{Z} + \sqrt{6}\,\mathbb{Z}$.

Proof. Since $P = (2,\ \sqrt{6}) = 2\,\mathcal{O}_K + \sqrt{6}\mathcal{O}_K$, it is clear that $2\,\mathbb{Z} + \sqrt{6}\,\mathbb{Z} \subseteq P$. To show the reverse inclusion, we express an arbitrary element of P in terms of $\alpha,\ \beta \in \mathcal{O}_K$, where $\alpha := a + b\sqrt{6}$ and $\beta := c + d\sqrt{6}$ for appropriate $a,\ b,\ c,\ d \in \mathbb{Z}$. In particular, any element of P can be expressed as

$$\begin{aligned} 2\alpha + \beta\sqrt{6} &= 2\,(a + b\sqrt{6}) + (c + d\sqrt{6})\,\sqrt{6} \\ &= 2\,(a + 3d) + (2b + c)\,\sqrt{6} \\ &= 2\,a' + b'\,\sqrt{6} \end{aligned}$$

where $a',\ b' \in \mathbb{Z}$. Thus, $P \subseteq 2\,\mathbb{Z} + \sqrt{6}\,\mathbb{Z}$. □

Observation 2. $Q = 3\,\mathbb{Z} + \sqrt{6}\,\mathbb{Z}$.

Proof. Since $Q = (3,\ \sqrt{6}) = 3\,\mathcal{O}_K + \sqrt{6}\mathcal{O}_K$, it is clear that $3\,\mathbb{Z} + \sqrt{6}\,\mathbb{Z} \subseteq Q$. To show the reverse inclusion, we express an arbitrary element of Q in terms of $\alpha,\ \beta \in \mathcal{O}_K$, where $\alpha := a + b\sqrt{6}$

and $\beta := c + d\sqrt{6}$ for appropriate $a, b, c, d \in \mathbb{Z}$. In particular, any element of Q can be expressed as

$$\begin{aligned} 3\alpha + \beta\sqrt{6} &= 3\,(a + b\sqrt{6}) + (c + d\sqrt{6})\,\sqrt{6} \\ &= 3\,(a + 2d) + (3b + c)\,\sqrt{6} \\ &= 3\,a' + b'\,\sqrt{6} \end{aligned}$$

where $a', b' \in \mathbb{Z}$. Thus, $Q \subseteq 3\,\mathbb{Z} + \sqrt{6}\,\mathbb{Z}$. □

Exercise III.1. Prove that the ideals P and Q are prime in $\mathcal{O}_K$.

a. P is prime in $\mathcal{O}_K$.

Proof. Since $P, I \lhd \mathcal{O}_K$ with $I \subseteq P$, the third isomorphism theorem for rings, Theorem [DF04, 7.8 (3)] implies that

$$\begin{aligned} (P/I) &\trianglelefteq (\mathcal{O}_K/I), \\ (2, \sqrt{6}) \,/\, (\sqrt{6}) &\trianglelefteq \mathbb{Z}[\sqrt{6}] \,/\, (\sqrt{6}), \\ 2\,\mathbb{Z} &\trianglelefteq \mathbb{Z}. \end{aligned}$$

This, together with the isomorphism theorem, further implies that

$$(\mathcal{O}_K/P) \cong (\mathcal{O}_K/I) \,/\, (P/I) \cong \mathbb{Z} \,/\, 2\mathbb{Z} \in \{\text{Integral Domains}\}.$$

Thus, $P \trianglelefteq \mathcal{O}_K$ is prime by Theorem [AW04, 1.5.5]. □

b. Q is prime in $\mathcal{O}_K$.

Proof. Since $Q, I \lhd \mathcal{O}_K$ with $I \subseteq Q$, the third isomorphism theorem for rings, Theorem [DF04, 7.8 (3)], implies that

$$\begin{aligned}(Q/I) &\trianglelefteq (\mathcal{O}_K/I),\\ (3,\ \sqrt{6})\ /\ (\sqrt{6}) &\trianglelefteq \mathbb{Z}[\sqrt{6}]\ /\ (\sqrt{6}),\\ 3\,\mathbb{Z} &\trianglelefteq \mathbb{Z}.\end{aligned}$$

This, together with the isomorphism theorem, further implies that

$$(\mathcal{O}_K/Q) \quad\cong\quad (\mathcal{O}_K/I)\ /\ (Q/I) \quad\cong\quad \mathbb{Z}\ /\ 3\mathbb{Z} \quad\in\ \{\text{Integral Domains}\}.$$

Thus, $Q \trianglelefteq \mathcal{O}_K$ is prime by Theorem [AW04, 1.5.5]. □

Exercise III.2. Verify the following about the inverses of $P,\ Q\ \trianglelefteq\ \mathcal{O}_K$:

a. $P^{-1} \;=\; \frac{1}{2}\cdot P$; see Example [AW04, 8.3.3].

Verification. To verify that the set given above is indeed the fractional ideal inverse of P in $\mathcal{F}(\mathcal{O}_K)$, we must show that its product with P yields all of $\mathcal{O}_K$. That is, we must show $P^{-1}\,P \;=\; \mathcal{O}_K$.

To do so, we first observe that

$$\begin{aligned}(\tfrac{1}{2}\cdot P)\ P \quad=\quad \tfrac{1}{2}\cdot P^2 \quad&=\quad (\{\tfrac{1}{2}\cdot\alpha\,\beta \quad|\quad \alpha,\ \beta\in P\})\\ &=\quad (\{\tfrac{1}{2}\cdot\alpha\,\beta \quad|\quad \alpha,\ \beta\in (2,\ \sqrt{6})\})\\ &=\quad (\tfrac{1}{2}\cdot 2^2,\quad \tfrac{1}{2}\cdot\sqrt{6}^2,\quad \tfrac{1}{2}\cdot 2\,\sqrt{6})\\ &=\quad (2,\ 3,\ \sqrt{6}).\end{aligned}$$

The above product of ideals will contain any $\mathcal{O}_K$-linear combination of $2,\ 3,\ \sqrt{6}\in\mathcal{O}_K$ which means that $1 \;=\; 3-2\in(\frac{1}{2}\cdot P)\ P$, verifying that $\frac{1}{2}\cdot P \;=\; P^{-1}$. □

b. $Q^{-1} \;=\; \frac{1}{3} \cdot Q.$ [analogous to proof in part **a.**]

Verification. To verify that the set given above is indeed the fractional ideal inverse of Q in $\mathcal{F}(\mathcal{O}_K)$, we must show that its product with Q yields all of $\mathcal{O}_K$. That is, we must show $Q^{-1}\, Q \;=\; \mathcal{O}_K$.
To do so, we first observe that

$$\begin{aligned}
(\tfrac{1}{3} \cdot Q)\; Q \quad &= \quad \tfrac{1}{3} \cdot Q^2 \\
&= \quad (\{\tfrac{1}{3} \cdot \alpha\, \beta \quad | \quad \alpha,\; \beta \in Q\}) \\
&= \quad (\{\tfrac{1}{3} \cdot \alpha\, \beta \quad | \quad \alpha,\; \beta \in (3,\; \sqrt{6})\}) \\
&= \quad (\tfrac{1}{3} \cdot 3^2, \quad \tfrac{1}{3} \cdot \sqrt{6}^2, \quad \tfrac{1}{3} \cdot 3\, \sqrt{6}) \\
&= \quad (3,\; 2,\; \sqrt{6}).
\end{aligned}$$

The above product of ideals will contain any $\mathcal{O}_K$-linear combination of $3,\; 2,\; \sqrt{6} \in \mathcal{O}_K$ which means that $1 \;=\; 3 - 2 \in (\frac{1}{3} \cdot Q)\; Q$, verifying that $\frac{1}{3} \cdot Q \;=\; Q^{-1}$. □

Exercise III.3. Verify that $P\; Q$ is the unique prime factorization of $I \trianglelefteq \mathcal{O}_K$.

Verification. Extraneous explanatory details are omitted from this arithmetic:

$$\begin{aligned}
P\; Q \quad = \quad (2,\; \sqrt{6})\; (3,\; \sqrt{6}) \quad &= \quad (6,\; 2\sqrt{6},\; 3\sqrt{6},\; 6) \\
&= \quad (\sqrt{6}^2,\; 2\sqrt{6},\; 3\sqrt{6}) \\
&= \quad (\sqrt{6})\; (\sqrt{6},\; 3,\; 2) \\
&= \quad (\sqrt{6}).
\end{aligned}$$

Uniqueness follows from the fact that K is a dedekind domain. □

Exercise III.4. Derive and verify that $\frac{1}{6} \cdot I$ is the fractional inverse of I.

Solution. Exercise III.3 implies $I \;=\; P\,Q,$ further implying the following arithmetic (in which extraneous explanatory details are omitted):

$$\begin{aligned} I^{-1} &= P^{-1}\,Q^{-1} \\ &= (\tfrac{1}{2} \cdot P)\,(\tfrac{1}{3} \cdot Q) \\ &= (\tfrac{1}{2})(\tfrac{1}{3}) \cdot (P\,Q) \\ &= \tfrac{1}{6} \cdot I \end{aligned}$$

To verify, $(\frac{1}{6} \cdot I)\,I \;=\; \frac{1}{6} \cdot I^2 \;=\; \frac{1}{6} \cdot (\sqrt{6}^2) \;=\; (1).$ □

EXERCISE IV.

Let A be a dedekind domain which is not a field; let $I,\ J \in \mathcal{F}(A) \setminus \{(0)\}$; let $N \in \mathcal{I}(A) \setminus \{(0)\}$; let $M \in \mathcal{F}(A)$; and let $K := \operatorname{Frac} A$.

Definition IV.1 (**Order of an Ideal w.r.t. a Prime Ideal**)**.** If A is dedekind, then any nonzero $I \in \mathcal{F}(A)$ can be expressed as a product of integral powers of finitely many prime ideals. In other words, any such fractional ideal can be written as

$$I \quad = \quad \prod_{i=1}^{n} {P_i}^{a_i} \qquad \text{where} \qquad a_i \in \mathbb{Z} \quad \text{for all} \quad 1 \leqslant i \leqslant n.$$

We define the **order of an ideal** I **with respect to a prime ideal** P_i in terms of the integral powers of prime ideals in the decomposition of I. That is, we define $\operatorname{ord}_{P_i} I \ := \ a_i$. For any prime ideal P such that $P \neq P_1, \ldots, P_n$ we define $\operatorname{ord}_P I \ := \ 0$. [AW04, Definition 8.4.1]

Definition IV.2 (**Order of an Element w.r.t. a Prime Ideal**)**.** For $\alpha \in K \setminus \{0\}$, we define the **order of an element** α **with respect to a prime ideal** P as $\operatorname{ord}_P \alpha \ := \ \operatorname{ord}_P\, (\alpha)$. [AW04, Definition 8.4.3]

Exercise IV. Prove that M is generated by at most two elements.

This proof follows that of Theorem [AW04, 8.5.1].

Proof. In the boundary cases, that is, when $M = \{0\}$ and $M = A$, we observe that $M = (0)$ and $M = (1)$, respectively. In these cases, M is generated by at most two elements, satisfying the claim we want to prove.
So, consider when $M \in \mathcal{F}(A) \setminus \{(0),\ (1)\}$ and let $\eta \in M$ such that $\eta \neq 0$ and such that $\eta \notin U(A)$ (i.e. $\eta \not\approx 1$). Since $\eta \in M$, then $(\eta) \subseteq M$,

implying that $M \mid (\eta)$. Thus, there exists some $N \in \mathcal{I}(A) \setminus \{(0)\}$ such that

$$M\ N \quad = \quad (\eta).$$

Let $P_1, \ldots, P_k \trianglelefteq A$ be distinct prime ideals such that, for all $1 \leqslant i \leqslant k$, the order with respect to P_i of either or both of M and MN is nonzero. There must be at least one such P_i for, otherwise, $\mathrm{ord}_P\ M = 0$ for all prime $P \trianglelefteq A$ implying that $M = (1) = A$, a case we have previously dealt with.

Taking $m_i := \mathrm{ord}_{P_i}\ M$, Theorem [AW04, 8.4.5] ensures the existence of an element $\mu \in K := \mathrm{Frac}\, A$ such that $\mathrm{ord}_{P_i}\ \mu = m_i$ for all $1 \leqslant i \leqslant k$ and such that $\mathrm{ord}_P\ \mu \geqslant 0$ for any $P \notin \{P_1, \ldots, P_k\}$. Further, for any such P, we have that $\mathrm{ord}_P\ M = 0$. Thus, $\mathrm{ord}_P\ \mu \geqslant \mathrm{ord}_P\ M$ *for all* prime ideals $P \trianglelefteq A$ which means that $M \mid (\mu)$ and, further, that $\mu \in M$. Now, since N is integral, then $MN \subseteq M$. So, $M + MN = M$ and

$$\begin{aligned}
\mathrm{ord}_{P_i}\ M + MN &= \mathrm{ord}_{P_i}\ M \\
&= \min\{\ \mathrm{ord}_{P_i}\ M, \quad \mathrm{ord}_{P_i}\ MN\ \} \\
&= \min\{\ \mathrm{ord}_{P_i}\ \mu, \quad \mathrm{ord}_{P_i}\ MN\ \} \\
&= \min\{\ \mathrm{ord}_{P_i}\ (\mu), \quad \mathrm{ord}_{P_i}\ MN\ \} \\
&= \mathrm{ord}_{P_i}\ (\mu)\ +\ MN
\end{aligned}$$

for all $1 \leqslant i \leqslant k$ by Theorem [AW04, 8.4.2 (b)]. If $P \notin \{P_1, \ldots, P_k\}$, then $\mathrm{ord}_P\ \mu \geqslant \mathrm{ord}_P\ MN$ because $\mathrm{ord}_P\ MN = 0$ for all such P. Thus,

$$\begin{aligned}
0 = \mathrm{ord}_P\ M &= \min\{\ \mathrm{ord}_P\ \mu, \quad \mathrm{ord}_P\ MN\ \} \\
&= \mathrm{ord}_P\ (\mu)\ +\ MN
\end{aligned}$$

by Theorem [AW04, 8.4.2 (b)]. So we have that

$$\operatorname{ord}_P M \quad = \quad \operatorname{ord}_P \ (\mu) + MN$$

for all prime ideals P, implying that $M = (\mu) + MN$. Finally, because $MN = (\eta)$, we conclude that $M = (\mu) + (\eta) = (\mu,\ \eta)$. □

Exercise V.

Let K be a number field of degree $n = [K:\mathbb{Q}]$ with associated number ring $\mathcal{O}_K$ and let $a \in \mathcal{O}_K$ denote an arbitrary integral element of K. Let $\alpha \in K$ denote an arbitrary field element of degree m over $\mathbb{Q}$ with minimal polynomial given by

$$\mathbf{m}(X) \quad := \quad X^m + a_{m-1}X^{m-1} + \cdots + a_0 \quad \in \mathbb{Q}[X].$$

We will denote the $n \times n$ matrix with entries $a_1, \ldots, a_n$ along the main diagonal by $\mathbf{D}(a_1, \ldots, a_n)$.

Exercise V.1. Prove that $\mathbf{N}\,(a\,\mathcal{O}_K) = \left| \mathbf{N}_{K/\mathbb{Q}}\, a \right|$.

Proof. Let $\{\varepsilon_1, \ldots, \varepsilon_n\}$ be an integral basis for K. Then $\{a\,\varepsilon_1, \ldots, a\,\varepsilon_n\}$ is a minimal basis for the principal ideal $a\,\mathcal{O}_K$, so

$$\begin{aligned}
\mathrm{disc}_{K/\mathbb{Q}}\, a\,\mathcal{O}_K &= \mathrm{disc}_{K/\mathbb{Q}}\,(a\,\varepsilon_1, \ldots, a\,\varepsilon_n) \\
&= \det\,(\sigma_i(a\,\varepsilon_j))^2 \\
&= \det\,(\sigma_i(a)\,\sigma_i(\varepsilon_j))^2 \\
&= \det\,(\mathbf{D}(\sigma_1(a), \ldots, \sigma_n(a))\,(\sigma_i(\varepsilon_j)))^2 \\
&= \det\,(\mathbf{D}(\sigma_1(a), \ldots, \sigma_n(a)))^2\, \det\,(\sigma_i(\varepsilon_j))^2 \\
&= (\sigma_1(a)\,\sigma_2(a)\,\cdots\,\sigma_n(a))^2\, \mathrm{disc}_{K/\mathbb{Q}}\,(\varepsilon_1, \ldots, \varepsilon_n) \\
&= \left(\mathbf{N}_{K/\mathbb{Q}}\, a\right)^2 (\mathrm{disc}\ K/\mathbb{Q}), \qquad \text{and thus}
\end{aligned}$$

$$\mathbf{N}\,(a\,\mathcal{O}_K) = \sqrt{\frac{\mathrm{disc}_{K/\mathbb{Q}}\,(a\,\mathcal{O}_K)}{\mathrm{disc}\,(K/\mathbb{Q})}} = \sqrt{\left(\mathbf{N}_{K/\mathbb{Q}}\, a\right)^2} = \left|\mathbf{N}_{K/\mathbb{Q}}\, a\right|.$$

$\square$

Exercise V.2. Prove that $\mathbf{N}\,(\alpha\,\mathcal{O}_K) = |\,a_0\,|^{(n/m)}$.

Proof. We know by Theorem [AW04, 6.3.2] that $m \mid n$. Setting $\alpha_1 := \alpha$, define $\alpha_2, \ldots, \alpha_m$ to be the Galois conjugates of α_1 so that

$$\mathbf{m}(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0 = (X-\alpha_1)\cdots(X-\alpha_m).$$

Then $a_0 = (-1)^m\,\alpha_1\,\cdots\,\alpha_m$. By Theorem [AW04, 6.3.2] the complete set of Galois conjugates of α_1 in K is

$$\alpha_1, \ldots, \alpha_1 \;,\; \alpha_2, \ldots, \alpha_2 \;, \ldots, \; \alpha_m, \ldots, \alpha_m,$$

where each α_i is repeated n/m times. Then

$$\begin{aligned} \mathbf{N}_{K/\mathbb{Q}}\alpha &= \alpha_1^{(n/m)}\,\cdots\,\alpha_m^{(n/m)} \\ &= (\alpha_1\,\cdots\,\alpha_m)^{(n/m)} \\ &= ((-1)^m\,a_0)^{(n/m)} \\ &= (-1)^n\,a_0^{(n/m)}, \end{aligned}$$

so by Exercise V.1 we have

$$\mathbf{N}\,(\alpha\,\mathcal{O}_K) = \left|\,\mathbf{N}_{K/\mathbb{Q}}\alpha\right| = \left|(-1)^n\,a_0^{(n/m)}\right| = |a_0|^{(n/m)}.$$

□

Now, let $K := \mathbb{Q}\big(\sqrt{2} + \sqrt{3}\,\big)$.

Exercise V.3. Show that $\mathbf{N}\,(\sqrt{2}\,\mathcal{O}_K) = 4$.

Proof. The minimal polynomial of $\sqrt{2}$ is $X^2 - 2$ and $[K : \mathbb{Q}] = 4$, so by Exercise V.2 we have $\mathbf{N}\,(\sqrt{2}\,\mathcal{O}_K) = |-2|^{(4/2)} = 4$. □

Exercise VI.

Consider the cubic number field $K := \mathbb{Q}(\sqrt[3]{2})$.

Exercise VI.1. Prove that $\operatorname{disc} K/\mathbb{Q} = -108$.

Not a proof. Example [AW04, 7.1.6] is very long, so I'll just note that it requires proving that $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ is an integral basis for $\mathcal{O}_K$ "manually" because the discriminant $\operatorname{disc}_{K/\mathbb{Q}} \sqrt[3]{2} = -108$ is not squarefree. □

Exercise VI.2. List all the rational primes which ramify in the extension $K/\mathbb{Q}$.

Solution. By Theorem [AW04, 10.1.5], a rational prime p ramifies in K if and only if it divides $\operatorname{disc} K/\mathbb{Q} = -108 = -2^2 \cdot 3^3$, so the rational primes which ramify in $K/\mathbb{Q}$ are 2 and 3. □

Exercise VI.3. Show that the splitting of $5 \in \mathbb{Q}$ in $K/\mathbb{Q}$ is given by $5\,\mathcal{O}_K = PQ$ where

$$P = (5, \sqrt[3]{2} + 2) \quad \text{and} \quad Q = (5, (\sqrt[3]{2})^2 + 3\sqrt[3]{2} + 4).$$

Proof. The minimal polynomial of $\sqrt[3]{2}$ is $X^2 - 3$. Then

$$X^3 - 2 \equiv (X+2)(X^2 + 3X + 4) \pmod 5,$$

so because both $X + 2$ and $X^2 + 3X + 4$ are irreducible modulo 5, we have by Theorem [AW04, 10.3.1] that $5\,\mathcal{O}_K = PQ$ as defined above. □

Exercise VI.4. Find the ramification indices $e_1,\ e_2$ and the inertial degrees $f_1,\ f_2$ associated to the splitting in Exercise VI.3

Solution. From the splitting $5\,\mathcal{O}_K = P^1Q^1$ it is clear that the ramification indices of P and Q are $e_1 = e_2 = 1$. By Theorem [AW04, 10.3.1] we have that $\mathbf{N}\,(P) = p^1$ and $\mathbf{N}\,(Q) = p^2$, so the inertial degrees of P and Q are $f_1 = 1$ and $f_2 = 2$, respectively. □

Exercise VII.

Let K be a square number field; let $\mathrm{cl}\#[\,K\,]$ denote its *class number*; let $\mathcal{O}_K$ be its associated square number ring; and let p be a rational prime. Recall that there exists a unique, squarefree $d \in \mathbb{Z}$ such that $K = \mathbb{Q}(\sqrt{d}\,)$ for any number field K of degree $[K:\mathbb{Q}] = 2$ by Theorem [AW04, 6.5.5].

Theorem VII.1 (**Lifting Rational Primes to SNRs**)**.** [AW04, Thm 10.2.1] A rational prime p will either **i.** split, **ii.** ramify or **iii.** remain inert when lifted to a square number ring. The behavior of ideals of $\mathcal{O}_K$ lying above p can be determined via the following criteria:

i. Split. We say p **splits** in K if $(p) = P\,Q$ where P and Q are distinct prime ideals of $\mathcal{O}_K$. In this case, the norms of the ideals are such that $\mathbf{N}(P) = \mathbf{N}(Q) = p$. Splitting occurs when

- **a.** $\underline{p = 2}$: $d \equiv 1 \pmod 8$; or
- **b.** $\underline{p > 2}$: $\left[\!\left[\frac{d}{p}\right]\!\right] = 1.$

ii. Ramify. We say p **ramifies** in K if $(p) = P^2$ where P is a prime ideal of $\mathcal{O}_K$. In this case, the norm of the ideal is such that $\mathbf{N}(P) = p$. Ramification occurs when

- **a.** $\underline{p = 2}$: $d \equiv 2$ or $3 \pmod 4$; or
- **b.** $\underline{p > 2}$: $\left[\!\left[\frac{d}{p}\right]\!\right] = 0$ (equivalently, $p \mid d$).

iii. Remain Inert. We say p **remains inert** in K if (p) is a prime ideal of $\mathcal{O}_K$. A rational prime remains inert when

- **a.** $\underline{p = 2}$: $d \equiv 5 \pmod 8$; or
- **b.** $\underline{p > 2}$: $\left[\!\left[\frac{d}{p}\right]\!\right] = -1.$

My solutions roughly follow the algorithm given in [AW04, §12.6, p. 315]. I do not reproduce the algorithm here, but I will state the observation preceding the algorithm in the text:

Remark VII.2 (**Class Number One Criterion**). We terminate the algorithm for determining the *ideal class group* of an algebraic number field K and conclude that $\mathrm{cl}\#[\,K\,] = 1$ if all prime ideals lying above rational primes $p \leqslant M_K$ are also principal.

The following solutions follow Examples [AW04, 12.6.1–3].

Exercise VII.1. Prove that $\mathrm{cl}\#\big[\,\mathbb{Q}(\sqrt{-19}\,)\,\big] = 1.$

Proof. Let $K := \mathbb{Q}(\sqrt{-19})$. That is, take $d = -19$. To compute the class number of K, we begin by attempting to determine its ideal class group. We reduce this process to determining *representatives* of ideal classes by bounding the number of rational primes that we will lift and factor in $\mathcal{O}_K$. Taking all possible products of prime ideals lying above the rational primes determined by the *minkowski bound* yields at least one representative for every ideal class.

S1. Compute minkowski constant. The minkowski constant (or minkowski bound) is an upper bound for the rational primes we consider when determining ideal classes of K. It depends on the degree of K and the number of real/complex conjugates of the generator of K as an extension of $\mathbb{Q}$. In particular, we use the following two auxiliary constants to compute the minkowski bound:

  i. Number of complex conjugate pairs of generator. In this case, K is an *imaginary square number field* which means that there is $s = 1$ complex conjugate pair and no real conjugates of $\sqrt{-19}$ in K.

ii. **Discriminant of extension.** Since $-19 \equiv 1 \pmod 4$, it follows that $\operatorname{disc}_{\mathbb{Q}} K = -19$.

Thus, the *minkowski bound* of K is

$$\begin{aligned} M_K &= \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}_{\mathbb{Q}} K|} \\ &= \left(\frac{2}{\pi}\right) \sqrt{19} \\ &< \frac{2}{3} \cdot 5 \\ &\approx 3.3. \end{aligned}$$

S2. Lift and factor rational primes. The rational primes $p \leqslant M_K$ are $p = 2$ and $p = 3$. For $p > 2$, we compute Legendre symbols and, in any case, we end up performing simple modular arithmetic to determine the behavior of rational primes in K.

a. $\underline{p = 3}$: Since $-19 = -18 - 1 \equiv 2 \pmod 3$, which is not a square modulo 3, the relevant Legendre symbol evaluates to

$$\left[\!\left[\frac{-19}{3}\right]\!\right] = -1$$

implying that the principal ideal $(3) \trianglelefteq \mathcal{O}_K$ is also prime.

b. $\underline{p = 2}$: Since $-19 \not\equiv 2$ or $3 \pmod 4$, we proceed to arithmetic modulo 8 to find that $-19 = -16 - 3 \equiv 5 \pmod 8$, implying that the principal ideal $(2) \trianglelefteq \mathcal{O}_K$ is also prime.

S3. (Apply Class Number One Criterion). Before proceeding, as the algorithm does, by computing products of the prime ideal factors of principal ideals generated by the indicated rational primes, we determine if K has class number one. Since both of the rational primes we considered remain inert in K, the principal ideals they generate are prime in $\mathcal{O}_K$. In other words, all prime ideals of $\mathcal{O}_K$ that lie above $p = 2, 3$ are all principal, implying that K satisfies the class number one criterion.

We now terminate the algorithm and conclude $\mathrm{cl}\#\,[\,\mathbb{Q}(\sqrt{-19}\,)\,] = 1.$ □

Exercise VII.2. Prove that $\mathrm{cl}\#\,[\,\mathbb{Q}(\sqrt{-163}\,)\,] = 1.$

Proof. Let $K := \mathbb{Q}(\sqrt{-163})$. That is, take $d = -163$.

S1. Compute minkowski constant. We proceed as above to compute the minkowski bound.

   i. Number of complex conjugate pairs of generator. In this case, K is an *imaginary square number field* which means that there is $s = 1$ complex conjugate pair and no real conjugates of $\sqrt{-163}$ in K.

   ii. Discriminant of extension. Since $-163 \equiv 1 \pmod 4$, it follows that $\mathrm{disc}_{\mathbb{Q}}\, K = -163$.

Thus, the *minkowski bound* of K is

$$\begin{aligned} M_K = \left(\frac{2}{\pi}\right)^s \sqrt{|\mathrm{disc}_{\mathbb{Q}}\, K|} = \left(\frac{2}{\pi}\right) \sqrt{163} &< \frac{2}{3}\sqrt{164} \\ &< \frac{4}{3}\sqrt{41} \\ &< \frac{4}{3}\cdot 7 \\ &< 10. \end{aligned}$$

S2. Lift and factor rational primes. The rational primes $p \leqslant M_K$ are $p = 2,\ 3,\ 5,\ 7$. For $p > 2$, we compute Legendre symbols and, in any case, we end up performing simple modular arithmetic to determine the behavior of rational primes in K.

a. $\underline{p=2}$: Since $-163 \not\equiv 2$ or $3 \pmod 4$, we proceed to find that $-163 = -160-3 \equiv 5 \pmod 8$, implying that the principal ideal $(2) \trianglelefteq \mathcal{O}_K$ is also prime.

b. $\underline{p=3}$: Since $-163 = -162-1 \equiv 2 \pmod 3$, which is not a square modulo 3, the relevant Legendre symbol evaluates to

$$\left[\!\left[\frac{-163}{3}\right]\!\right] = -1$$

implying that the principal ideal $(3) \trianglelefteq \mathcal{O}_K$ is also prime.

c. $\underline{p=5}$: Since $-163 = -160-3 \equiv 2 \pmod 5$, which is not a square modulo 5, the relevant Legendre symbol evaluates to

$$\left[\!\left[\frac{-163}{5}\right]\!\right] = -1$$

implying that the principal ideal $(5) \trianglelefteq \mathcal{O}_K$ is also prime.

d. $\underline{p=7}$: Since $-163 = -161-2 \equiv 5 \pmod 7$, which is not a square modulo 7, the relevant Legendre symbol evaluates to

$$\left[\!\left[\frac{-163}{7}\right]\!\right] = -1$$

implying that the principal ideal $(7) \trianglelefteq \mathcal{O}_K$ is also prime.

S3. (Apply Class Number One Criterion). Since all of the rational primes we considered remain inert in K, the principal ideals they generate are prime in $\mathcal{O}_K$. In other words, all prime ideals of $\mathcal{O}_K$ that lie above rational primes $p \leqslant M_K$ are principal, implying that K satisfies the class number one criterion.

We now terminate the algorithm and conclude $\text{cl}\#\left[\,\mathbb{Q}(\sqrt{-163}\,)\,\right] \;=\; 1.$ $\square$

Exercise VII.3. Prove that $\text{cl}\#\left[\,\mathbb{Q}(\sqrt{23}\,)\,\right] \;=\; 1.$

Proof. Let $K \;:=\; \mathbb{Q}(\sqrt{23})$. That is, take $d \;=\; 23.$

S1. Compute minkowski constant. We proceed as above to compute the minkowski bound.

i. Number of complex conjugate pairs of generator. Now, K is a *real square number field.* Thus, there are $r \;=\; 2$ real conjugates and $s = 0$ complex conjugate pairs of $\sqrt{23}$ in K.

ii. Discriminant of extension. Since $23 \equiv 3 \pmod 4$, it follows that $\text{disc}_{\mathbb{Q}}\, K \;=\; 4 \cdot 23 \;=\; 92.$

Thus, the *minkowski bound* of K is

$$\begin{aligned} M_K \;&=\; \left(\frac{2}{\pi}\right)^s \sqrt{|\text{disc}_{\mathbb{Q}}\, K|} \\ &=\; \sqrt{92} \\ &<\; 10 \end{aligned}$$

S2. Lift and factor rational primes. The rational primes $p \leqslant M_K$ are $p = 2,\ 3,\ 5,\ 7.$ For $p > 2,$ we compute Legendre symbols and, in any case, we end up performing simple modular arithmetic to determine the behavior of rational primes in K.

a. $\underline{p = 3}$: Since $23 \;=\; 21 + 2 \;\equiv\; 2 \pmod 3$, which is not a square modulo 3, the relevant Legendre symbol evaluates to

$$\left[\!\!\left[\frac{23}{3}\right]\!\!\right] \;=\; -1$$

implying that the principal ideal $(3) \trianglelefteq \mathcal{O}_K$ is also prime.

b. $\underline{p = 5}$: Since $23 = 20 + 3 \equiv 3 \pmod 5$, which is not a square modulo 5, the relevant Legendre symbol evaluates to

$$\left[\!\!\left[\frac{23}{5}\right]\!\!\right] = -1$$

implying that the principal ideal $(5) \trianglelefteq \mathcal{O}_K$ is also prime.

c. $\underline{p = 7}$: Since $23 = 21 + 2 \equiv 2 \pmod 7$, is a square modulo 7, the relevant Legendre symbol evaluates to

$$\left[\!\!\left[\frac{23}{7}\right]\!\!\right] = 1$$

implying that (7) splits in $\mathcal{O}_K$. Following the proof of Theorem [AW04, 10.2.1], we reach the conclusion given in [AW04, §10.2, p. 245] and observe that, since $7 \nmid 23$, then

$$(7) = \left(7,\ x + \sqrt{23}\right)\left(7,\ x - \sqrt{23}\right)$$

for x a square modulo 7 which is equivalent to $23 \equiv 2 \pmod 7$. Thus, $x = 3$ or $x = 4$.
However, since $7 - (3 + \sqrt{23}) = 4 - \sqrt{23}$ and since $(4 - \sqrt{23})\,(-4 - \sqrt{23}) = 7$, it follows that

$$\left(7,\ 3 + \sqrt{23}\right) = \left(7,\ 4 - \sqrt{23}\right) = \left(4 - \sqrt{23}\right) \trianglelefteq \mathcal{O}_K$$

is principal. We similarly deduce that
$\left(7,\ 3 - \sqrt{23}\right) = \left(4 + \sqrt{23}\right) \trianglelefteq \mathcal{O}_K$ is principal.

d. $\underline{p = 2}$: Since $23 \equiv 3 \pmod 4$, we know that $p = 2$ ramifies in K. As in the previous case, we follow the proof of Theorem [AW04, 10.2.1] to find that

$$(2) \quad = \quad \left(2,\ 1+\sqrt{23}\right)^2 .$$

Now, taking $a \in \mathbb{Z}$, we observe that

$$(a+\sqrt{23})\,(a-\sqrt{23}) \quad = \quad a^2 - 23$$

and, setting this equal to 2, we deduce that $a^2 = 25$ and, further, that $a = 5$. In other words, $(5+\sqrt{23}) \mid 2$ in $\mathcal{O}_K$. Further, since $2\cdot 2 \ + \ 1\,(1+\sqrt{23}) \ = \ 5+\sqrt{23}$, implying that $5+\sqrt{23} \in \left(2,\ 1+\sqrt{23}\right)$, we deduce that

$$\left(2,\ 1+\sqrt{23}\right) \quad = \quad \left(5+\sqrt{23}\right) \quad \trianglelefteq \ \mathcal{O}_K$$

is principal.

S3. (Apply Class Number One Criterion). The rational primes we considered which do not remain inert either split or ramify into prime ideals which are also principal. In other words, all prime ideals of $\mathcal{O}_K$ that lie above rational primes $p \leqslant M_K$ are principal implying that K satisfies the class number one criterion.

We now terminate the algorithm and conclude $\mathrm{cl}\#\left[\ \mathbb{Q}(\sqrt{23}\,)\ \right] \ = \ 1.$ □

Exercise VIII.

Let $\mathbf{CL}[\,K\,]$ denote the *ideal class group* of an algebraic number field K.

"So, are we automatons?

Yes. But we are magnificent automatons!"

– Ab-Bot (*Futurama*)

It is now time to perform the glorious group ritual to completion. That is, we now perform the algorithm to determine the ideal class group of an algebraic number field *without terminating to conclude that the number field has class number one*! ~~In other words, shit just got *real*.~~ [AW04, Example 12.6.5]

Exercise VIII. Prove that $\mathbf{CL}\left[\,\mathbb{Q}(\sqrt{-14}\,)\,\right] \cong \mathbb{Z}/4\mathbb{Z}$.

Proof. Let $K := \mathbb{Q}(\sqrt{-14})$. That is, take $d = -14$. We reduce the task of determining all ideal classes of K to determining *representatives* of ideal classes by bounding the number of rational primes that we will lift and factor in $\mathcal{O}_K$. Taking all possible products of prime ideals lying above the rational primes determined by the *minkowski bound* yields at least one representative for every ideal class.

S1. Compute minkowski constant. The minkowski constant (or minkowski bound) is an upper bound for the rational primes we consider when determining ideal classes of K. It depends on the degree of K and the number of real/complex conjugates of the generator of K as an extension of $\mathbb{Q}$; it also depends on the discriminant of K. In particular, we use the following auxiliary constants to compute the minkowski bound:

i. Number of complex conjugate pairs of generator. Since K is an *imaginary square number field*, there is $s = 1$ complex conjugate pair and no real conjugates of $\sqrt{-14}$ in K.

ii. Discriminant of extension. Since

$$-14 = -12 - 2 \equiv 2 \pmod{4},$$

it follows that $\operatorname{disc}_{\mathbb{Q}} K = 4\,(-14) = -56.$

Thus, the *minkowski bound* of K is

$$\begin{aligned} M_K &= \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}_{\mathbb{Q}} K|} = \left(\frac{2}{\pi}\right) \sqrt{56} < \frac{1}{3}\sqrt{4 \cdot 56} \\ &< \frac{1}{3}\sqrt{224} \\ &< \frac{1}{3} \cdot 15 \\ &< 5. \end{aligned}$$

S2. Lift and factor rational primes. The rational primes $p \leqslant M_K$ are

a. $p = 3$ and **b.** $p = 2$.

i. Compute Legendre Symbols. We now compute Legendre symbols using simple modular arithmetic to determine the behavior of rational primes in K using the criteria given in Theorem VII.1.

a. $\underline{p = 3}$: Since $-14 = -12 - 2 \equiv 1 \pmod{3}$ is a square modulo 3, the relevant Legendre symbol evaluates to

$$\left[\!\left[\frac{-14}{3}\right]\!\right] = 1$$

implying that $(3) = P_1\, P_2$ for prime ideals $P_1,\ P_2 \trianglelefteq \mathcal{O}_K$. In other words, $p = 3$ splits in K.

b. $\underline{p=2}$: Since $-14 = -12-2 \equiv 2 \pmod 4$, we deduce that $p=2$ ramifies in K. In other words, $(2) = P^2$ for $P \trianglelefteq \mathcal{O}_K$ a prime ideal.

ii. Determine prime ideals lying above rational primes. We now find explicit forms of the prime ideals $P,\ P_1,\ P_2 \trianglelefteq \mathcal{O}_K$ lying above the rational primes $p = 2,\ 3$.

a. $\underline{p=3}$: In this case, $p=3$ splits into prime ideal factors

$$(3) = P_1\ P_2 = \big(3,\ 1+\sqrt{-14}\big)\,\big(3,\ 1-\sqrt{-14}\big)\,,$$

as 1 is the only square modulo 3. see [AW04, §10.2, p. 245]

b. $\underline{p=2}$: Since $-14 = -12-2 \equiv 2 \pmod 4$, we deduce that $p=2$ ramifies as

$$(2) = P^2 = \big(2,\ \sqrt{-14}\big)^2$$

for $P \trianglelefteq \mathcal{O}_K$ prime. see [AW04, §10.2, p. 245]

S3. Products of prime ideal class representatives. Let's get this bread! We found the prime ideals of $\mathcal{O}_K$ which lie above the rational primes determined by the minkowski constant. They are

$$\begin{aligned} P &= \big(2,\ \sqrt{-14}\big)\,, \\ P_1 &= \big(3,\ 1+\sqrt{-14}\big)\,, \qquad \text{and} \\ P_2 &= \big(3,\ 1-\sqrt{-14}\big)\,. \end{aligned}$$

Now, we cleverly observe (~~or read in the textbook~~) that

$$3-(1+\sqrt{-14}) = 2-\sqrt{-14} =:\ \alpha$$

is contained in both P and P_1.

Recalling that $\boxed{\text{“} \textit{to contain is to divide} \text{”}}$ in the context of nonzero integral ideals of algebraic number fields, we now have that $P \mid (\alpha)$ and $P_1 \mid (\alpha)$. Because P_1 and P are prime ideals lying above distinct rational primes, they are themselves distinct. Thus, their product is such that $P_1 \, P \mid (\alpha)$ implying that there exists some integral prime $M \trianglelefteq \mathcal{O}_K$ such that $P_1 \, P \, M = (\alpha)$. Taking norms of both sides of the preceding ideal equality, we have

$$\begin{aligned} \mathbf{N}(P_1)\,\mathbf{N}(P)\,\mathbf{N}(M) &= \mathbf{N}(\alpha) \\ 3 \cdot 2 \;\; \mathbf{N}(M) &= 2^2 + 14 = 18 \\ \text{implying that} \quad \mathbf{N}(M) &= 3, \end{aligned}$$

further implying that $\mathbf{N}(M) = 3$ and that $M \trianglelefteq \mathcal{O}_K$ is a prime ideal lying above 3 by Theorem [AW04, 10.1.2]. This means that exactly one of **(1)** or **(2)** must hold:

(1) $\underline{M = P_2}$: If this were the case, it would imply that

$$P \, P_1 \, P_2 = P \, (3) = (\alpha)$$

which would further imply that $(3) \mid \left(2 - \sqrt{-14}\right)$, an impossibility.

(2) Thus, $M = P_1$ (meaning that $(\alpha) = P_1^2 \, P$).

Considering the above ideal equality in the ideal class group, we have

$$\begin{aligned} \mathbf{1} &= [\,(\alpha)\,] \\ &= [\,{P_1}^2 \, P\,] = [\,P_1\,]^2 \, [\,P\,] \\ \text{implying that} \quad [\,P\,] &= [\,P_1\,]^2 \, [\,P\,]^2 = [\,P_1\,]^2 \end{aligned}$$

as $P^2 = (2)$ is principal. In other words, we have $\boxed{[\,P\,] = [\,P_1\,]^2.}$ Now, since $P^2 = (2)$ is principal, we also have $[\,P\,]^2 = \mathbf{1}$. The above imply that $\boxed{[\,P_1\,]^4 = \mathbf{1},}$ and further imply that $\boxed{[\,P_1\,]^3 = [\,P_2\,].}$ Thus, every ideal class for K can be expressed as powers of the ideal class $\boxed{[\,P_1\,].}$

Now, to put our minds at ease, we verify that the above powers of $[\,P_1\,]$ are unique elements of $\mathbf{CL}\left[\,\mathbb{Q}(\sqrt{-14})\,\right]$. We verify the following three cases:

(1) $\underline{[\,P_1\,] \neq [\,P_1\,]^3}$: If this were the case, it would imply that

$$\begin{aligned} [\,P_1\,] &= [\,P_1\,]^3 \\ [\,P_1\,]^2 &= [\,P_1\,]^4 \\ [\,P_1\,]^2 &= \mathbf{1} \end{aligned}$$

and further imply that $[\,P\,] = \mathbf{1}$, which cannot be true as $P = \left(2,\ \sqrt{-14}\right)$ is not principal. $\square$

(2) $\underline{[\,P_1\,] \neq [\,P_1\,]^2}$: If this were the case, it would imply that

$$\begin{aligned} [\,P_1\,] &= [\,P_1\,]^2 \\ [\,P_1\,]^3 &= [\,P_1\,]^4 \\ [\,P_1\,]^3 &= \mathbf{1} \end{aligned}$$

further imply that $[\,P_2\,] = \mathbf{1}$. In other words, this would mean that $P_2 = \left(3,\ 1 - \sqrt{-14}\right)$ is principal.
Suppose that it were principal. That is, assume $P_2 = \left(a + b\sqrt{-14}\right)$ for some $a,\ b \in \mathbb{Z}$. Then $\mathbf{N}(P_2) = 3 = a^2 + 14b^2$, which would be impossible. $\square$

(3) $\underline{[\ P_1\ ]^2 \neq [\ P_1\ ]^3}$: If this were the case, it would imply that

$$[\ P_1\ ]^2 = [\ P_1\ ]^3$$
$$[\ P_1\ ]^3 = [\ P_1\ ]^4$$
$$[\ P_1\ ]^3 = \mathbf{1},$$

which we have already shown cannot be true. □

We reassure ourselves that we need not fret over the possibility that $[\ P_1\ ] = \mathbf{1}$ as the justification for P_1 being non-principal is analogous to the proof of Case **(2)**. Thus, $\mathbf{CL}\left[\ \mathbb{Q}(\sqrt{-14})\ \right] = \mathbb{Z}/4\mathbb{Z}$. □

Exercise IX.

Let K be a number field with $[K : \mathbb{Q}] = n$ and let $\mathcal{O}_K$ denote its associated number ring.

Exercise IX.1. Prove that $\mathcal{O}_K$ contains only finitely many roots of unity.

Proof. If $\zeta_k \in \mathcal{O}_K$ is a primitive k^{th} root of unity, then $\mathbb{Q}(\zeta_k) \subseteq K$. So

$$\phi(k) = [\mathbb{Q}(\zeta_k) : \mathbb{Q}] \leq [K : \mathbb{Q}] = n$$

and, by Lemma [AW04, 13.5.2], we must then have that $k \leq 2n^2$.
Thus $\mathcal{O}_K$ contains only finitely many roots of unity. □

Exercise IX.2. If n is odd, prove that the only roots of unity in $\mathcal{O}_K$ are 1 and -1.

Proof. If $\zeta_k \in \mathcal{O}_K$ is a primitive k^{th} root of unity, then $\mathbb{Q}(\zeta_k) \subseteq K$. So

$$\phi(k) = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] \quad \text{divides} \quad [K : \mathbb{Q}] = n.$$

By Lemma [AW04, 13.5.6], $\phi(k)$ is even for $k \geq 3$. So, because n is odd, we must have $k = 1,\ 2$. Thus the only roots of unity in $\mathcal{O}_K$ are $\zeta_1 = 1$ and $\zeta_2 = -1$. □

Exercise IX.3. If $n = 4$, prove that the only possible roots of unity in $\mathcal{O}_K$ other than 1 and -1 are powers of ζ_i for

$$i \in \{3, 4, 5, 6, 8, 10, 12\}.$$

Proof. If $\zeta_k \in \mathcal{O}_K$ is a primitive k^{th} root of unity, then $\mathbb{Q}(\zeta_k) \subseteq K$. So

$$\phi(k) \quad = \quad [\mathbb{Q}(\zeta_p) : \mathbb{Q}] \qquad \text{divides} \qquad [K : \mathbb{Q}] \quad = \quad 4$$

and, thus, $\phi(k) = 1,\ 2,$ or 4. By Lemmas [AW04, 13.5.3–5] the only values which satisfy these conditions are $1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 8,\ 10,$ and 12, so the only possible roots of unity in $\mathcal{O}_K$ other than 1 and -1 are powers of ζ_i for $i \in \{3, 4, 5, 6, 8, 10, 12\}$. □

EXERCISE X.

We remind the reader that *cyclotomic number fields* are rational extensions of the form $\mathbb{Q}(\zeta_k)$ where ζ_k denotes a primitive k^{th} root of unity. One may also call such a number field "*the* k^{th} *cyclotomic (number) field*".

Definition X.1 (Number Ring—Cyclotomic). Let K denote the k^{th} cyclotomic number field. I call the ring of integers of K a **cyclotomic number ring**. As it is well established that $\{1, \zeta, \ldots, \zeta^{(\varphi(k)-1)}\}$ is an integral basis for the k^{th} cyclotomic field, we settle for *defining* cyclotomic number rings to be such that $\mathcal{O}_K := \mathbb{Z}[\zeta_k]$.

Exercise X. Let $K := \mathbb{Q}(\zeta_p)$ for an odd prime p. Describe $U(\mathcal{O}_K)$.

Note that the following solution follows the proof of Theorem [ME05, 8.1.10]. The following claim may hold true under less restrictive conditions (i.e. considering a cyclotomic field generated by an arbitrary odd root of unity), but we will not overcomplicate things by introducing additional prime factors to the integers under consideration.

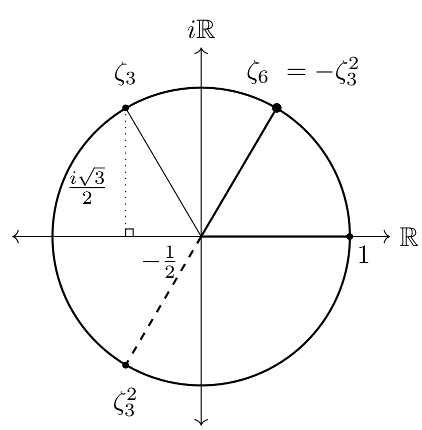

Figure 1: $\zeta_3 \mapsto \zeta_3^2 \mapsto \zeta_6$

Claim X.1. $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{2p})$.

Proof. For p an odd prime we know $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{2p})$ since $\zeta_{2p} = -\zeta_{2p}^{p+1} = -\zeta_p^{\frac{p+1}{2}}$. This elegant observation is illustrated via example in the figure. However, we also give the following verification:

$$-\zeta_p^{\frac{p+1}{2}} \quad = \quad -\left(e^{\frac{2\pi i}{p}}\right)^{\frac{p+1}{2}} \quad = \quad -\exp\left(\frac{2\pi i}{p}\cdot\frac{p+1}{2}\right)$$
$$= \quad -\exp\left(\frac{2\pi i}{p}\cdot\frac{p}{2} \;+\; \frac{2\pi i}{p}\cdot\frac{1}{2}\right)$$
$$= \quad -\exp\left(\frac{2\pi i}{p}\cdot\frac{p}{2}\right)\exp\left(\frac{2\pi i}{p}\cdot\frac{1}{2}\right)$$
$$= \quad -\exp\left(\pi i\right)\cdot\exp\left(\frac{2\pi i}{2p}\right)$$
$$= \quad 1\cdot\zeta_{2p} \quad = \quad \zeta_{2p}.$$

□

Consequently, it suffices to prove the following:

Claim X.2. Let $K := \mathbb{Q}(\zeta_m)$ for m even. Then the roots of unity contained in $\mathcal{O}_K$ are $\{1,\ \zeta_m,\ \zeta_m^2\ ,\ldots,\ \zeta_m^{m-1}\}$.

Proof. Suppose that $\zeta_k \in \mathcal{O}_K$ is a primitive k^{th} root of unity such that $k \nmid m$. Without loss of generality we may take $\zeta_m = e^{\frac{2\pi i}{m}}$ and $\zeta_k = e^{\frac{2\pi i}{k}}$. Let $d := \gcd(m,\ k)$, let $\ell := \operatorname{lcm}(m,\ k)$ and let $m',\ k' \in \mathbb{Z}$ such that $m = d\,m'$ and $k = k'\,d$. Then $\gcd(m',\ k') = 1$, so there exist $x,\ y \in \mathbb{Z}$ such that $x\ m' \ +\ y\ k' \ = \ 1.$ Then

$$\zeta_m^y\cdot\zeta_k^x \quad = \quad \exp\left(\frac{2\pi i}{m}\right)^y\cdot\exp\left(\frac{2\pi i}{k}\right)^x \quad = \quad \exp\left(\frac{2\pi i}{m}\cdot y \;+\; \frac{2\pi i}{k}\cdot x\right)$$
$$= \quad \exp\left(\frac{2\pi i}{d}\cdot\left(\frac{y}{m'} \;+\; \frac{x}{k'}\right)\right)$$
$$= \quad \exp\left(\frac{2\pi i}{d}\cdot\frac{x\ m' \;+\; y\ k'}{m'\ k'}\right)$$
$$= \quad \exp\left(\frac{2\pi i}{m'\ k'\ d}\right)$$
$$= \quad \exp\left(\frac{2\pi i}{\ell}\right),$$

so $\mathcal{O}_K$ contains a primitive ℓ^{th} root of unity, $\zeta_\ell := \zeta_m^y \cdot \zeta_k^x$. Then $L := \mathbb{Q}(\zeta_\ell) \subseteq K$, so

$$\varphi(\ell) = [L : \mathbb{Q}] \leqslant [K : \mathbb{Q}] = \varphi(m).$$

However, because m is *even* and because m *properly* divides ℓ we must have that $\varphi(m)$ properly divides $\varphi(\ell)$, and in particular $\varphi(m) < \varphi(\ell)$. This is a contradiction, so no such ζ_k exists. Then the only roots of unity contained in $\mathcal{O}_K$ are powers of ζ_m. The result follows. □

Together, the previous two claims imply that for $K = \mathbb{Q}(\zeta_p)$, the roots of unity contained in $\mathcal{O}_K$ are

$$\{\pm 1, \ \pm\zeta_p, \ \pm\zeta_p^2, \ldots, \ \pm\zeta_p^{p-1}\} = \{1, \ \zeta_{2p}, \ \zeta_{2p}^2, \ldots, \ \zeta_{2p}^{2p-1}\}.$$

To finish the exercise we require the following:

Claim X.3. Let K be an arbitrary number field with $[K : \mathbb{Q}] = n$, let

$$\sigma_i : K \hookrightarrow \mathbb{C} \qquad \text{for} \qquad i = 1, 2, \ldots, n$$

denote the n distinct embeddings of K into $\mathbb{C}$, and let $|\cdot|$ denote the norm in $\mathbb{C}$. If $\alpha \in \mathcal{O}_K$ is such that $|\sigma_i(\alpha)| = 1$ for all $1 \leqslant i \leqslant n$, then α is a root of unity.

Proof. For $k > 0$, define the polynomials

$$\varphi_k(X) := \prod_{i=1}^{n} (X - \sigma_i(\alpha)^k).$$

These polynomials cannot all be distinct because $|\sigma_i(\alpha)^k| = 1$, so suppose that $\varphi_m(X) = \varphi_k(X)$ for some $m < k$. The roots of these polynomials must coincide, so if $\alpha^m = \alpha^k$ then it is clear that $\alpha^{k-m} = 1$. Otherwise we may relabel the embeddings so that

$$\begin{aligned}
\sigma_1(\alpha)^m &= \sigma_2(\alpha)^k, \\
\sigma_2(\alpha)^m &= \sigma_3(\alpha)^k, \\
&\vdots \\
\sigma_{n-1}(\alpha)^m &= \sigma_n(\alpha)^k, \\
\sigma_n(\alpha)^m &= \sigma_1(\alpha)^k.
\end{aligned}$$

Then $\sigma_1(\alpha)^{m^n} = \sigma_2(\alpha)^{km^{n-1}} = \sigma_3(\alpha)^{k^2 m^{n-2}} = \cdots = \sigma_1(\alpha)^{k^n}$, so $\sigma_1(\alpha^{k^n - m^n}) = \sigma_1(\alpha)^{k^n - m^n} = 1$ and, thus, $\alpha^{k^n - m^n} = 1$. This implies that α is a root of unity. □

We can now prove the following:

Claim X.4. $U(\mathcal{O}_K) = \{\pm 1,\ \pm\zeta_p,\ \pm\zeta_p^2\ , \ldots,\ \pm\zeta_p^{p-1}\} \cong \mathbb{Z}/2p\mathbb{Z}$.

Proof. The group isomorphism is clear because the first claim implies that

$$\{\pm 1,\ \pm\zeta_p,\ \pm\zeta_p^2\ , \ldots,\ \pm\zeta_p^{p-1}\} = \{1,\ \zeta_{2p},\ \zeta_{2p}^2\ , \ldots,\ \zeta_{2p}^{2p-1}\} \cong \mathbb{Z}/2p\mathbb{Z}.$$

Further, it is clear that $U(\mathcal{O}_K) \supseteq \{\pm 1,\ \pm\zeta_p,\ \pm\zeta_p^2\ , \ldots,\ \pm\zeta_p^{p-1}\}$, so it remains to be shown that $U(\mathcal{O}_K) \subseteq \{\pm 1,\ \pm\zeta_p,\ \pm\zeta_p^2\ , \ldots,\ \pm\zeta_p^{p-1}\}$.
Suppose that $\varepsilon \in U(\mathcal{O}_K)$ and let

$$\sigma_i\ :\ K \hookrightarrow \mathbb{C} \qquad \text{for} \qquad i = 1,\ 2, \ldots,\ p-1$$

denote the $p-1$ distinct embeddings of K into $\mathbb{C}$. Then $|\varepsilon/\overline{\varepsilon}| = 1$.

Further we must have that

$$|\sigma_i(\varepsilon/\overline{\varepsilon})| \quad = \quad |\sigma_i(\varepsilon)/\sigma_i(\overline{\varepsilon})| \quad = \quad 1 \qquad \text{for all} \qquad 1 \leqslant i \leqslant p-1.$$

Then $\varepsilon/\overline{\varepsilon} \;=\; \pm\zeta_p^k$ is a root of unity by the previous claim.
Because $\{1,\ \zeta_p,\ \zeta_p^2\ ,\ldots,\ \zeta_p^{p-2}\}$ is an integral basis for $\mathcal{O}_K$, there exist $a_0,\ a_1,\ldots,\ a_{p-2} \in \mathbb{Z}$ such that $\varepsilon = \sum_{i=0}^{p-2} a_i\ \zeta_p^i$ and, further, that

$$\overline{\varepsilon} \quad = \quad \sum_{i=0}^{p-2} a_i\ \zeta_p^{-i}.$$

Then

$$\begin{aligned} \varepsilon^p \quad &\equiv \quad \left(\sum_{i=0}^{p-2} a_i\ \zeta_p^{\ i}\right)^p \quad \equiv \quad \sum_{i=0}^{p-2} a_i \pmod p \qquad \text{and} \\ \overline{\varepsilon}^p \quad &\equiv \quad \left(\sum_{i=0}^{p-2} a_i\ \zeta_p^{-i}\right)^p \quad \equiv \quad \sum_{i=0}^{p-2} a_i \quad \equiv \quad \varepsilon^p \pmod p. \end{aligned}$$

If $\varepsilon \;=\; -\zeta_p^k \cdot \overline{\varepsilon}$ then $\varepsilon^p \;\equiv\; -\varepsilon^p \pmod p$ implying that

$$\begin{aligned} \varepsilon^p \quad &\equiv \quad -\varepsilon^p \pmod p \\ 2\ \varepsilon^p \quad &\equiv \quad 0 \pmod p, \end{aligned}$$

and, further, that $\varepsilon^p \equiv 0 \pmod p$. But then $\varepsilon^p \in p\ \mathcal{O}_K$ which contradicts the assumption that ε is a unit. Thus $\varepsilon/\overline{\varepsilon} \;=\; \zeta_p^k$.
Now, let $r \in \mathbb{Z}$ such that $2r \;\equiv\; k \pmod p$ and let $\delta \;:=\; \varepsilon\ \zeta_p^{-r} \in U(\mathcal{O}_K)$.
Then $\overline{\delta} \;=\; \overline{\varepsilon}\ \zeta_p^r \;=\; \varepsilon\ \zeta_p^{r-k} \;=\; \varepsilon\ \zeta_p^{-r} \;=\; \delta,$ so $\delta \in (\mathbb{R} \cap U(\mathcal{O}_K)) \;=\; \{\pm 1\}$ and thus $\varepsilon \;=\; \pm\zeta_p^k \;\in \{\pm 1,\ \pm\zeta_p,\ \pm\zeta_p^2\ ,\ldots,\ \pm\zeta_p^{p-1}\}$.

□

References

[AW04] Şaban Alaca and Kenneth S. Williams. *Introductory algebraic number theory.* Cambridge University Press, Cambridge, 2004.

[DF04] D.S. Dummit and R.M. Foote. *Abstract Algebra.* Wiley, 2004.

[ME05] M. Ram Murty and Jody Esmonde. *Problems in algebraic number theory*, volume 190 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 2005.