Math 129 Problem Set 4

Lev Kruglyak

February 28, 2022

For any number field K, we'll use $\mathcal{O}_K$ to denote the ring of integers of K, i.e. $\mathcal{O}_K = \mathbb{A} \cap K$. Also let $\Delta(\cdots)$ be the discriminant. We'll use Δ_K to mean the discriminant of a number field K.

Problem 2.40. In the notation of Theorem 2.13, establish the formula

$$\Delta(\alpha) = (d_1 d_2 \cdots d_{n-1})^2 \Delta_K.$$

Notice that by Theorem 2.13, we have

$$\Delta_K = \Delta\left(1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{n-1}(\alpha)}{d_{n-1}}\right).$$

By properties of discriminant and determinant, multiplying the matrix by $d_1 d_2 \cdots d_{n-1}$ gives us $\Delta(1, f_1(\alpha), \dots, f_{n-1}(\alpha)) = (d_1 d_2 \cdots d_{n-1})^2 \Delta_K$. We next claim that $1, f_1(\alpha), \dots, f_{n-1}(\alpha)$ is an integral basis for $\mathbb{Z}[\alpha]$. This follows by induction and because f_i are all monic of degree i, so we can show that α^i can be generated by $1, f_1(\alpha), \dots, f_i(\alpha)$. Thus $\Delta(\alpha) = \Delta(1, f_1(\alpha), \dots, f_{n-1}(\alpha))$, completing the proof.

Problem 2.43. Let $f(x) = x^5 + ax + b$ where $a, b \in \mathbb{Z}$ and assume that $f(x)$ is irreducible in $\mathbb{Q}[x]$. Let α be a root of $f(x)$.

(a) Show that $\Delta(\alpha) = 4^4 a^5 + 5^5 b^4$.

(b) Suppose $\alpha^5 = \alpha + 1$. Show that $\mathcal{O}_{\mathbb{Q}[\alpha]} = \mathbb{Z}[\alpha]$.

(a) First note that $\alpha^5 + a\alpha + b = 0$ so $\alpha^4 = \frac{a\alpha+b}{-\alpha}$. Thus $f'(\alpha) = \frac{5a\alpha+5b}{-\alpha} + a\alpha = \frac{4a\alpha+5b}{-\alpha}$. By Theorem 2.8, and because $d \equiv 1 \mod 4$ we have

$$\Delta(\alpha) = \mathrm{N}^{\mathbb{Q}[\alpha]}(f'(\alpha)) = \frac{\mathrm{N}^{\mathbb{Q}[\alpha]}(4a\alpha + 5b)}{\mathrm{N}^{\mathbb{Q}[\alpha]}(-\alpha)}.$$

Note that $4a\alpha + 5b$ is a root of the irreducible polynomial $g_1(x) = \left(\frac{x-5b}{4a}\right)^5 + a\left(\frac{x-5b}{4a}\right) + b$, so by Theorem 2.4 and Vieta's formulas,

$$\begin{aligned}\mathrm{N}^{\mathbb{Q}[\alpha]}(4a\alpha + 5b) &= (-1)^5 \left(\frac{x^0 \text{ coefficient of } g_1}{x^5 \text{ coefficient of } g_1}\right) = \frac{\left(-\frac{5b}{4a}\right)^5 - \frac{5b}{4} + b}{\left(\frac{1}{4a}\right)^5} \\ &= -5^5 b^5 - 5 \cdot 4^4 a^5 b + 4^5 a^5 b = 4^4 a^5 b + 5^5 b^5.\end{aligned}$$

Similarly, $-\alpha$ is the roof of the irreducible polynomial $g_2(x) = x^5 + ax - b$ so $\mathrm{N}^{\mathbb{Q}[\alpha]}(-\alpha) = b$. Thus $\Delta(\alpha) = 4^4a^5 + 5^5b^4$.

(b) First we'll show that $f(x) = x^5 - x - 1$ is irreducible, since α is a root. Clearly if $f(x)$ were reducible, it would not have any linear factors because $f(x) \equiv 1 \mod 2$ so it has no integral roots. So it must have one quadratic factor and one cubic factor. Let $g(x)$ be the irreducible quadratic factor of $f(x)$. Then $\mathbb{F}_5[x]/(g(x)) \cong \mathbb{F}_5[\alpha] \cong \mathbb{F}_{25}$. However in $\mathbb{F}_{25}$, $\alpha^25 = \alpha$, yet $\alpha^25 = (\alpha^5)^5 = (\alpha+1)^5 = \alpha^5 + 1 = \alpha + 2$, so $\alpha + 2 = \alpha$. This is impossible, so $f(x)$ must be irreducible.

Then by (a), $\Delta(\alpha) = 2869$ which is squarefree, so by Theorem 2.9, $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ is an integral basis for $\mathbb{Q}[\alpha]$. Thus $\mathcal{O}_{\mathbb{Q}[\alpha]} = \mathbb{Z}[\alpha]$.

Problem 3.1. For any integral domain R, prove that the following conditions are equivalent:

1. Every ideal is finitely generated.
2. Every increasing sequence of ideals $I_1 \subset I_2 \subset \cdots$ is eventually constant.
3. Every non-empty set S of ideals of R has a maximal member; i.e. $\exists M \in S$ such that $M \subset I \in S$ implies that $M = I$.

(1) $\implies$ (2): Suppose $I_1 \subset I_2 \subset \cdots$ is an increasing chain of ideals of R. Then $\bigcup_i I_i$ is an ideal in R, so it must be finitely generated by (1), say $\bigcup_i I_i = (r_1, \ldots, r_n)$. We can assume without loss of generality that all of the inclusions are proper. Say $r_1 \in I_1$. Then I_2 must contain one of the other r_i or else $I_1 = I_2$, say $r_2 \in I_2$. Then by induction $I_n = (r_1, \ldots, r_n)$ so $I_m = I_n$ for all $m > n$. So the sequence is eventually constant.

(2) $\implies$ (3): S can be given the structure of a partially ordered set, and (2) implies that every chain has an upper bound, so by Zorn's lemma there must be some maximal element satisfying the conditions of (3).

(3) $\implies$ (1): Let I be an ideal in R. Consider the family of ideals $\{(S)\}_{S \text{ finite subset of } I}$ where (S) is the ideal generated by the set $S \subset I$. By (3), there must be some maximal member of this family, say $M = (r_1, \ldots, r_n)$. Then for any element $r \in I$, we have $M \subset (r_1, \ldots, r_n, r)$ so $r \in M$. This means that $I = M$ so I is finitely generated.

Problem 3.2. Prove that every finite integral domain is a field.

Let K be a finite integral domain and let $\alpha \in K$ be a nonzero element. Consider the set $S_\alpha = \{1, \alpha, \alpha^2, \ldots\} \subset K$. Since K is an integral domain, $0 \notin S_\alpha$. So by the pigeonhole principle there must be some $n > m$ such that $\alpha^n = \alpha^m \neq 0$. Then $\alpha^{n-m} = 1$ and so α^{n-m-1} is a multiplicative inverse for α. Thus K is a field.

Problem 3.7. Show that if I, J are ideals in a commutative ring such that $1 \in I + J$, then $1 \in I^n + J^m$ for all m, n.

Since $1 \in I + J$, there is an $\alpha \in I$ and $\beta \in J$ such that $1 = \alpha + \beta$. Then

$$\begin{aligned}
1 = (\alpha+\beta)^{n+m} &= \sum_{k=0}^{n+m} \binom{n+m}{k} \alpha^k \beta^{n+m-k} \\
&= \underbrace{\sum_{k=0}^{n} \binom{n+m}{n-k} \alpha^{n-k}\beta^{m+k}}_{J^m} + \underbrace{\sum_{k=1}^{m} \binom{n+m}{k+n} \alpha^{k+n}\beta^{m-k}}_{I^n}.
\end{aligned}$$

Thus $1 \in I^n + J^m$.

Problem 3.9. Let $K \subset L$ be number fields

(a) Let $I, J \subset \mathcal{O}_K$ be ideals and suppose $I \cdot \mathcal{O}_L \mid J \cdot \mathcal{O}_L$. Show that $I \mid J$.

(b) Show that for each ideal I in $\mathcal{O}_K$, we have $I = I \cdot \mathcal{O}_L \cap \mathcal{O}_K$.

(c) Characterize those ideals I of $\mathcal{O}_L$ such that $I = (I \cap \mathcal{O}_K) \cdot \mathcal{O}_L$.

(a) Factor $I = \prod_i \mathfrak{p}_i^{e_i}$ and $J = \prod_i \mathfrak{p}_i^{r_i}$ where only a finite number of the e_i, r_j are nonzero. Then we have $I \cdot \mathcal{O}_L = \prod_i (\mathfrak{p}_i \cdot \mathcal{O}_L)^{e_i}$ and $J \cdot \mathcal{O}_L = \prod_i (\mathfrak{p}_i \cdot \mathcal{O}_L)^{r_i}$. However by Theorem 3.20, each $\mathfrak{p}_i \cdot \mathcal{O}_L = \prod_{j \in S_i} \mathfrak{P}_j^{s_j}$ where $\mathfrak{P}_j$ is a prime in $\mathcal{O}_L$ and $S_i \cap S_n = \varnothing$ for $i \neq n$. Thus

$$I \cdot \mathcal{O}_L = \prod_i (\mathfrak{p}_i \cdot \mathcal{O}_L)^{e_i} = \prod_i \prod_{j \in S_i} \mathfrak{P}_j^{e_i s_j}$$

and likewise for J. Thus if $I \cdot \mathcal{O}_L \mid J \cdot \mathcal{O}_L$ then $e_i s_j \leq r_i s_j$ for all i and $j \in S_i$. Since S_i are nonempty, this means that $e_i \leq r_i$ for all i. However this implies that $I \mid J$ so we are done.

(b) Again factor $I = \prod_i \mathfrak{p}_i^{e_i}$, setting $I \cdot \mathcal{O}_L = \prod_i \prod_{j \in S_i} \mathfrak{P}_j^{e_i s_j}$. Then note that by Theorem 3.19 $\mathfrak{P}_j \cap \mathcal{O}_K = \mathfrak{p}_i$ whenever $j \in S_i$. This means that $\left(\prod_{j \in S_i} \mathfrak{P}_j^{s_j}\right) \cap \mathcal{O}_K = \mathfrak{p}_i$ and so by extension $I \cdot \mathcal{O}_L \cap \mathcal{O}_K = I$.

(c) We claim that this is only true if $I = J \cdot \mathcal{O}_L$ for some ideal $J \subset \mathcal{O}_K$. Indeed if $J \subset \mathcal{O}_K$ is an ideal then by (b), $(J \cdot \mathcal{O}_K \cap \mathcal{O}_K) \cdot \mathcal{O}_L = J \cdot \mathcal{O}_L = I$. Conversely, if I is some ideal in $\mathcal{O}_L$ satisfying $I = (I \cap \mathcal{O}_K) \cdot \mathcal{O}_L$ then $J = (I \cap \mathcal{O}_K)$. This completes the proof.