MAT415 Assignment 2 Solutions

October 24, 2020

Problem 1 (Exercise 1.38 on Pg. 20)**.** *Let I be a nonzero ideal in a Dedekind ring R with factorization $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ into prime ideals. Then:*

a) $I^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$.

b) $II^{-1} = R$.

Solution. a) By definition, $I^{-1} = \{x \in K \colon xI \subset R\}$. First, we note that

$$\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} I = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} \mathfrak{p}_1 \cdots p_r = (\mathfrak{p}_1^{-1} \mathfrak{p}_1) \cdots (\mathfrak{p}_r^{-1} \mathfrak{p}_r) \subset R \cdots R \subset R.$$

This shows that $\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} \subset I^{-1}$.

On the other hand, by definition, we have $I^{-1}I = I^{-1} \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset R$. By Corollary 1.36, we know that $\mathfrak{p}\,\mathfrak{p}^{-1} = R$ for a prime ideal $\mathfrak{p}$ of Dedekind domain R. Multiplying both sides of $I\,\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset R$ by $\mathfrak{p}_r^{-1}$, we find:

$$I^{-1} \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1} = I^{-1} \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1} R \subset I^{-1} \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1} (\mathfrak{p}_r \mathfrak{p}_r^{-1}) \subset \mathfrak{p}_r^{-1}.$$

We proceed by successively multiplying both sides by $\mathfrak{p}_{r-1}^{-1}, \cdots, \mathfrak{p}_1^{-1}$, to find $I^{-1} \subset \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$.

We conclude that $I^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$ as required.

b) By Corollary 1.36, we know that $\mathfrak{p}\,\mathfrak{p}^{-1} = R$ for a prime ideal $\mathfrak{p}$ of Dedekind domain R. Using part (a), we find that

$$II^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} = (\mathfrak{p}_1 \mathfrak{p}_1^{-1}) \cdots (\mathfrak{p}_r \mathfrak{p}_r^{-1}) = R \cdots R = R$$

as required.

□

Problem 2 (Exercise 1.44 on Pg. 22)**.** *One can give an equivalent definition of* $\mathrm{Cl}(R)$ *without ever mentioning fractional ideals, as follows. We say that two ideals I, J of R are equivalent (and write $I \sim J$) if there exists nonzero elements a, b of R such that $aI = bJ$.*

a) Prove that $\sim$ defines an equivalence relation.

b) If $I \sim I'$ and $J \sim J'$, show that $IJ \sim I'J'$. Deduce that there is a natural group structure on the set of equivalence classes of nonzero ideals.

c) Prove that the group of equivalence classes of nonzero ideals of R is isomorphic to the ideal class group $\mathrm{Cl}(R)$.

Solution. a) To show that $\sim$ defines an equivalence relation, we must show that it is reflexive, symmetric and transitive. The fact that $\sim$ is symmetric and reflexive is immediate from the definition. To show that it is also transitive, suppose that $I \sim J$ and $J \sim K$ for ideals I, J, K of R. This means that there exists nonzero elements a, b, c, d of R such that $aI = bJ$ and $cJ = dK$. But then $caI = cbJ = bcJ = bdK$. Therefore $I \sim K$ and $\sim$ is transitive. Therefore, $\sim$ is an equivalence relation.

b) Suppose that $I \sim I'$ and $J \sim J'$. Then there exists some non-zero elements a, b, c, d of R such that $aI = bI'$ and $cJ = dJ'$. Then $acIJ = bdI'J'$. Thus $IJ \sim I'J'$.

Write the equivalence class of a non-zero ideal I under $\sim$ as $[I]$. The operation on the equivalence classed of non-zero ideals is $[I][J] = [IJ]$. The operation is clearly associative, has identity $[(1)] = [R]$. To see that every ideal has an inverse is a bit trickier. By Problem 1, we have that I^{-1} is a *fractional* ideal of R which has the property that $I^{-1}I = R$. Now, take an element r such that $rI^{-1} \subset R$ (any non-zero element of I works). Then rI^{-1} is an ideal of R and we have

$$rI^{-1}I = rR.$$

Therefore, $[rI^{-1}]$ is the inverse of $[I]$.

Therefore, we have a natural group structure on the set of equivalence classes of nonzero ideals. We call this group X.

c) Consider the map

$$\Phi \colon X \to \mathrm{Cl}(R)$$

given by $[I] \mapsto [I]$ sending the ideal class of I under $\sim$ to the equivalence class of the ideal I (considered now as a fractional ideal) in the ideal class group. This map is well defined because if $I \sim I'$, then $aI = bI'$ for some non-zero elements a, b of R, and so $(a/b)I = I'$, whence I and I' are equal in the ideal class group, and so $\Phi([I]) = \Phi([I'])$. The map Φ is a homomorphism because the operation in X and in the class group are both induced by multiplication of ideals. To see that it is injective, suppose that $\Phi([I]) = [(1)]$. Then $I = (\alpha)$ for some non-zero $\alpha \in K$. But since K is the fraction field of R, we can write $\alpha = \frac{a}{b}$ for some non-zero a, b in R. But then $bI = aR$ and so $[I] = [R] = [(1)]$. This shows that Φ is injective. To see that it is surjective, we just need to show that every fractional ideal is equivalent to an ideal of R in the class group. Let J be a fractional ideal. By the definition of fractional ideal, we can find a non-zero element $r \in R$ such that $rJ \subset R$. Then rJ is an ideal of R which we can call I and we have

$$rJ = I.$$

Therefore, $[J] = \Phi([I])$ and we conclude that Φ is surjective. Thus, we have shown that Φ is an isomorphism.

□

Problem 3 (Exercise 2.7 on Pg. 36)**.** *Let α be an algebraic integer of degree n, and let $f(x)$ be its minimal polynomial over $\mathbb{Q}$. Define the discriminant of α, denoted $\Delta(\alpha)$, to be the discriminant of the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ for $\mathbb{Q}(\alpha)/\mathbb{Q}$, and let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α.*

a) Show that

$$\Delta(\alpha) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\binom{n}{2}} N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(f'(\alpha)).$$

b) *Suppose α is a root of the polynomial $f(x) = x^n + ax + b$, where a, $b \in \mathbb{Z}$ are chosen so that $f(x)$ is irreducible. Use part a) to show that*

$$\Delta(\alpha) = (-1)^{\frac{n(n-1)}{2}} \left((-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}\right)$$

In particular, show that if $f(x) = x^2 + ax + b$ then $\Delta(\alpha) = a^2 - 4b$, an $\Delta(x) = x^3 + ax + b$ then $\Delta(\alpha) = -4a^3 - 27b^2$.

Solution. a) The second equality follows from the definition of the norm. For the first equality, we have that $\Delta(\alpha)$ is the determinant of the following matrix:

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots \alpha_2^{n-1} \\ & & \vdots & \\ 1 & \alpha_n & \alpha_n^2 & \cdots \alpha_n^{n-1} \end{pmatrix}.$$

This matrix is a Vandermonde matrix and it's determinant is given by the formula

$$\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$$

(see the Wikipedia page on the Vandermonde matrix for some nice proofs of this identity). On the other hand,

$$\prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n} \left(\prod_{i \neq j} (\alpha_i - \alpha_j) \right).$$

In the inner product, you need to make 0, 1, $\ldots$, $n-1$ sign changes when i is respectively equal to 1, 2, $\ldots$, n to make it equal to the determinant of the Vandermonde matrix. Therefore, $\Delta(\alpha)$ and $\prod_{i=1}^n f'(\alpha_i)$ differ by $(-1)^{\frac{n(n-1)}{2}}$ which gives the first equality.

b) From part a), it suffices to show that $\prod_{i=1}^n f'(\alpha_i) = (-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}$. Now, $f'(x) = nx^{n-1} + a$ and so $f'(\alpha_i) = n\alpha_i^{n-1} + a$. So $\prod_{i=1}^n f'(\alpha_i) = \prod_{i=1}^n (n\alpha_i^{n-1} + a)$. But we know that α_i are the roots of $f(x)$. In particular, $\alpha_i^n = -a\alpha_i - b$ and so $\alpha_i^{n-1} = -a - \frac{b}{\alpha_i}$. So the product above becomes:

$$\begin{aligned}
\prod_{i=1}^{n} (n\alpha_i^{n-1} + a) &= \prod_{i=1}^{n} (-na - \frac{nb}{\alpha_i} + a) \\
&= \prod_{i=1}^{n} \frac{1}{\alpha_i} (-(n-1)a\alpha_i - nb) \\
&= \frac{(-1)^n}{b} \prod_{i=1}^{n} (n-1)a \left(-\frac{nb}{(n-1)a} - \alpha_i \right) \\
&= \frac{(-1)^n}{b} (n-1)^n a^n f\left(-\frac{nb}{(n-1)a} \right) \\
&= \frac{(-1)^n}{b} (n-1)^n a^n \left(\left(-\frac{nb}{(n-1)a} \right)^n + a \left(-\frac{nb}{(n-1)a} \right) + b \right) \\
&= n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} n a^n + (-1)^n (n-1)^n a^n
\end{aligned}$$

$$\begin{aligned} &= n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n(n-(n-1)) \\ &= n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n, \end{aligned}$$

as required. If we substitute $n = 2$ in the formula above, we find $f(x) = x^2 + ax + b$ and $\Delta(\alpha) = -(-a^2 + 4b) = a^2 - 4b$. If we substitute $n = 3$, we find $f(x) = x^3 + ax + b$ and $\Delta(\alpha) = -(4a^3 + 27b^2) = -4a^3 - 27b^2$.

□

Problem 4 (Exercise 2.8 on Pg. 36)**.**

1. *Find an integral basis for the ring of integers of $\mathbb{Q}(\theta)$, where θ is a root of the polynomial $x^3 - 2x + 3$.*

2. *Find an integral basis for the ring of integers of $\mathbb{Q}(\theta)$, where θ is a root of the polynomial $x^3 - x - 4$.*

Solution. 1. Let $f(x) = x^3 - 2x + 3$. By Problem 3, the discriminant of $f(x)$ is -211. Now, 211 is prime and therefore $\{1, \theta, \theta^2\}$ is an integral basis for the ring of integers of $\mathbb{Q}(\theta)$.

2. Let $f(x) = x^3 - x - 4$. By Problem 3, the discriminant of $f(x)$ is $-428 = -4 \times 107$. If $\mathcal{O}_K \neq \mathbb{Z}[\theta]$, then by Lemma 2.3, the index of $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$ must be 2. If that's the case, by Lemma 2.5, $\mathcal{O}_K$ must contain one of $\frac{1}{2}$, $\frac{\theta}{2}$, $\frac{\theta^2}{2}$, $\frac{1+\theta}{2}$, $\frac{1+\theta^2}{2}$, $\frac{\theta+\theta^2}{2}$, $\frac{1+\theta+\theta^2}{2}$. The minimal polynomials of $\frac{1}{2}$, $\frac{\theta}{2}$, $\frac{1+\theta}{2}$ don't have integer coefficients. You can also check fairly easily that the minimal polynomial of $\frac{\theta^2}{2}$ does not have integer coefficients. We will check that $\frac{\theta+\theta^2}{2}$ does actually have integer coefficients. For this purpose, let's find the linear dependence between 1, $\frac{\theta+\theta^2}{2}$, $\left(\frac{\theta+\theta^2}{2}\right)^2$, and $\left(\frac{\theta+\theta^2}{2}\right)^3$. To do so, let's expand and simplify both $\left(\frac{\theta+\theta^2}{2}\right)^2$ and $\left(\frac{\theta+\theta^2}{2}\right)^3$ using the fact that $\theta^3 = x + 4$ coming from $f(x)$. We have:

$$\begin{aligned} \left(\frac{\theta+\theta^2}{2}\right)^2 &= \frac{\theta^4}{4} + \frac{\theta^3}{2} + \frac{\theta^2}{4} \\ &= \frac{\theta^2 + 4\theta}{4} + \frac{\theta + 4}{2} + \frac{\theta^2}{4} \\ &= \frac{\theta^2}{2} + \frac{3\theta}{2} + 2. \end{aligned}$$

Furthermore, we have:

$$\begin{aligned} \left(\frac{\theta+\theta^2}{2}\right)^3 &= \left(\frac{\theta+\theta^2}{2}\right)^2 \left(\frac{\theta+\theta^2}{2}\right) \\ &= \left(\frac{\theta^2}{2} + \frac{3\theta}{2} + 2\right)\left(\frac{\theta+\theta^2}{2}\right) \\ &= \frac{\theta^3}{4} + \frac{3\theta^2}{4} + \theta + \frac{\theta^4}{4} + \frac{3\theta^3}{4} + \theta^2 \\ &= \frac{\theta+4}{4} + \frac{3\theta^2}{4} + \theta + \frac{\theta^2 + 4\theta}{4} + \frac{3\theta + 12}{4} + \theta^2 \\ &= 2\theta^2 + 3\theta + 4. \end{aligned}$$

We must now find $a, b, c \in \mathbb{Q}$ such that $\left(\frac{\theta+\theta^2}{2}\right)^3 + a\left(\frac{\theta+\theta^2}{2}\right)^2 + b\left(\frac{\theta+\theta^2}{2}\right) + c = 0$. By the calculations above, this is the same as solving the system:

$$\begin{aligned} 2 + \frac{a}{2} + \frac{b}{2} &= 0 \\ 3 + \frac{3a}{2} + \frac{b}{2} &= 0 \\ 4 + 2a + c &= 0 \end{aligned}$$

This system has solution $(a, b, c) = (-1, -3, -2)$. Therefore, $\frac{\theta+\theta^2}{2}$ is a root of the polynomial $x^3 - x^2 - 3x - 2$ and as a result belongs to $\mathcal{O}_K$. We find that $\left\{1, \theta, \frac{\theta+\theta^2}{2}\right\}$ has discriminant -107. As this is square-free, we have found an integral basis.

□

Problem 5 (Exercise 2.18 on Pg. 42). *Show that every nonzero prime ideal* $\mathfrak{p}$ *of* $\mathcal{O}_K$ *lies over a unique prime number* p.

Solution. Since $\mathfrak{p}$ is non-zero, it contains a non-zero element α. Since α is an algebraic integer, it is the root of a monic polynomial in $\mathbb{Z}$, and we can write:

$$\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0$$

for some $a_i \in \mathbb{Z}$. But then $a_n \in \mathfrak{p}$. We can then factor a_n into primes in $\mathbb{Z}$, $a_n = p_1p_2\cdots p_l$. But since $\mathfrak{p}$ is a prime ideal it must contain at least one of those primes. Therefore, $\mathfrak{p}$ lies over at least one prime number. If $\mathfrak{p}$ contained two distinct primes p, q of $\mathbb{Z}$, then it would contain also contain $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$ and thus it would contain 1. Since prime ideals are proper, this would be a contradiction. Therefore, every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lies over a unique prime number p and thus $\mathfrak{p} \cap \mathbb{Z} = (p)$. □

Problem 6 (Exercise 2.25 on Pg. 43). *Factor the ideals* (2), (3), *and* (7) *into prime ideals in* $R = \mathbb{Z}[\sqrt[3]{2}]$.

Solution. By Proposition 2.10 in Baker's notes, $\mathbb{Z}[\sqrt[3]{2}]$ is the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$. This question is now easy to do by applying Kummer's Factorization Theorem, Lemma 2.15, because our ring is monogenic. It thus suffices to find the factorisation of the polynomial $f(x) = x^3 - 2$ into irreducible modulo 2,3, and 7. Modulo 2, $f(x) \equiv x^3 \pmod 2$ and so we have $(2) = (2, \sqrt[3]{2})^3$. Modulo 3, $f(x) \equiv (x+1)^3 \pmod 3$ and so we have $(3) = (3, \sqrt[3]{2}+1)^3$. Modulo 7, $f(x)$ does not have a root. As a result, it is irreducible, and so (7) is a prime ideal.

Remark 7. Over finite fields, there is a recursive algorithm that allows you to find all irreducible polynomials of degree d. Indeed, write down all the monic polynomials of degree d. There are finitely many since the base field is finite. For each of those, check using the Euclidean algorithm whether it is divisible by an irreducible polynomial of degree strictly less than d. If it is, discard it. If it is not, then it is irreducible. This way, you have written a list of the degree d irreducible polynomials.

Using the lists of irreducible polynomials of degree at most d you have built, you can factor any degree d polynomial into irreducibles by using the following algorithm. Take a polynomial f of degree d. Without loss of generality, we can assume it is monic (otherwise you divide it by the leading coefficient). Then, check with your list if it is irreducible. If not, you can find an irreducible factor of degree strictly less than d, say g_1. Then you can now repeat the process for f/g_1, $f/(g_1g_2)$ etc to find all the irreducible factors of f.

□