MATH110BH Homework 4

Boran Erol

February 2024

1 Problem 1

Lemma 1.1. Let $R = \mathbb{Z}[\sqrt{-5}]$. The ideal I generated by 2 and $1 + \sqrt(5)$ is not principal.

Proof. Since every multiple 2 and $1 + \sqrt{5}$ has even norm, $3 \notin I$. Therefore, $I \neq R$.

By contradiction, assume $d \in R$ such that $(d) = (2, 1 + \sqrt{5})$. Then, $d \mid 2$ and $d \mid 1 + \sqrt{5}$. Then, $N(d) \mid 4$ and $N(d) \mid 6$. Then, $N(d) = 1$ or $N(d) = 2$. Since no element of R satisfies $N(d) = 2$, $N(d) = 1$. Then, d is a unit, which is a contradiction. □

2 Problem 2

Lemma 2.1. $\mathbb{Z}[\sqrt{5}]$ is not a PID.

Proof. Notice that $4 = 2 \times 2 = (1 + \sqrt{5})(1 - \sqrt{5})$. Notice that $\mathbb{Z}[\sqrt{5}]$ doesn't have elements with norm equal to 2 or 3. Therefore, 2, $1 + \sqrt{5}$ and $1 - \sqrt{5}$ are all irreducible. Thus, $\mathbb{Z}[\sqrt{5}]$ is not a UFD, so it can't be a PID. □

3 Problem 3

Lemma 3.1. Let p be a prime number such that $p \equiv 3 \pmod 4$. Then, p is prime in $\mathbb{Z}[i]$.

Proof. Notice $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(x^2+1)/(p) \simeq \mathbb{Z}[x]/(p)/(x^2+1) \simeq \mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$.If $\mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$ is a field, (p) is maximal in $\mathbb{Z}[i]$ and therefore (p) is prime in $\mathbb{Z}[i]$. Thus, it suffices to show that $\mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$ is a field. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, $\mathbb{Z}/p\mathbb{Z}[x]$ is a PID. Therefore, it suffices to check that x^2+1 is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$. This holds if and only if x^2 is a quadratic residue modulo p, which is true if and only if $p \equiv 1 \pmod 4$. □

4 Problem 4

Lemma 4.1. Let p be a prime number such that $p \equiv 1 \pmod 4$. Then, p is not prime in $\mathbb{Z}[i]$.

Proof. Since $p \equiv 1 \pmod 4$, $\exists x \in \mathbb{Z} : x^2 \equiv -1 \pmod p \implies p \mid x^2 + 1 = (x-i)(x+i)$. Therefore, to prove that p is not prime in $\mathbb{Z}[i]$, it suffices to show that $p \nmid x - i$ and $p \nmid x + i$. Suppose that $p(a + bi) = x \pm i$. Then, $pa \mid x \implies x \equiv 0 \pmod p$, which implies $p = x$ or $x = 0$, which is a contradiction. □

Lemma 4.2. Let p be a prime number such that $p \equiv 1 \pmod 4$. Then, $\exists a, b \in \mathbb{Z} : p = a^2 + b^2$.

Proof. Since p is not prime in $\mathbb{Z}[i]$, there is some non-unit $x + yi$ with $x, y \in \mathbb{Z}$ that properly divides p. Then, the norm of $x + yi$ also properly divides p's norm. In other words $x^2 + y2$ properly divides p^2. Then, $x^2 + y^2 = 1$ or $x^2 + y^2 = p$. $x^2 + y^2 = 1$ can't be true since $x + yi$ is not a unit. Therefore, $x^2 + y^2 = p$. □

5 Problem 5

Lemma 5.1. Let R be a PID and let p be a prime element of R. Then, pR is a maximal ideal.

Proof. Suppose p is a prime element of R. Then, the ideal pR is maximal in the set of all principal ideals in R. Since R is a PID, pR is just a maximal ideal. $\square$

6 Problem 6

Lemma 6.1. Let S, T be Noetherian rings and let $R = S \times T$ be the product ring where addition and multiplication are defined component-wise. Then, R is also Noetherian.

Proof. Recall from a previous homework exercise that every ideal of R corresponds to $I \times J$ where I is an ideal of S and J is an ideal of T. Since both I and J are finitely generated, $I \times J$ is also finitely generated. Thus, every ideal of R is finitely generated. $\square$

7 Problem 7

Definition 1. An integral domain R is called a **Bezout domain** if every ideal generated by two elements is a principal ideal.

Lemma 7.1. Let R be ring. R is a UFD if and only if R is a Noetherian Bezout domain.

Proof. The forward implication is trivial. Let R be a PID. Then, every ideal in R is finitely generated since it's principal. This holds for ideals generated by two elements as well. Therefore, R is Noetherian and a Bezout domain.

Let's now prove the converse of the statement. Let R be a Noetherian Bezout domain and I be an ideal of R. Since R is Noetherian, I is generated by finitely many elements $a_1, ..., a_n$. We'll now induct on n to show that I is a principal ideal. The case with $n = 1$ is trivial and the case with $n = 2$ follows from the fact that R is a Bezout domain. Now, assume the statement holds for some $n \in \mathbb{N}$ and let I be an ideal generated by $a_1, a_2, ..., a_n, a_{n+1}$. By the inductive hypothesis, the ideal generated by $a_1, a_2, ..., a_n$ is principal and thus there exists some $\alpha \in R$ that generates it. Then, $I = (\alpha, a_{n+1})$. Since R is a Bezout domain, it follows that I is principal and we conclude our proof. $\square$

8 Problem 8

Lemma 8.1. Let $R_1 \subset R_2 \subset ...$ be a chain of countably many subrings of a ring R such that $R = \bigcup R_i$. Suppose that all the R_i are UFDs and any prime element in every R_i is prime in R_{i+1}. Then, R is a UFD.

Proof. Let $r \in R$. Then, $r \in R_i$ for some $i \in \mathbb{N}$. Then, $r = c_1 \times ... \times cn$ where c_i is an irreducible element of R_i. Therefore, it suffices to show that c_i is irreducible in R. Let $c_i = uv$ for some $u, v \in R$. Then, $u, v \in R_j$ for some j by taking the maximum. Then, u or v is a unit in R_j. Since a unit in a smaller ring is a unit in the larger ring, u or v is a unit in R. Also notice that c_i doesn't become a unit in R since that would imply that it's a unit in some R_j, which contradicts our assumption that irreducibles stay irreducible.

Now, suppose by contradiction that factorization is not unique. Then, there is some $x \in R$ that has two different prime factorizations, i.e. $x = a_1 a_2 ... a_n = b_1 b_2 ... b_m$. Since a_i and b_j are all in R, they are all contained in some R_i and R_j. By taking the maximum of all of these indices, we get some R_i such that all a_i and b_i are in R_i and are prime in R_i. However, this contradicts the fact that R_i is a UFD. $\square$

9 Problem 9

Lemma 9.1. The polynomial ring $\mathbb{Z}[x_1, x_2, ...]$ in countably many variables is a UFD but not a Noetherian ring.

Proof. Notice that $\mathbb{Z}[x_1, x_2, ...] = \bigcup R_n$ where $R_n = \mathbb{Z}[x_1, x_2, ..., x_n]$. Then, $R_i \subset R_{i+1}$ and f prime in $R_i \implies x$ is prime in R_{i+1}. Thus, by Problem 9, $\mathbb{Z}[x_1, x_2, ...]$ is a UFD.

Now, let I_n be the ideal generated by $(x_1, ..., x_n)$. Clearly, $I_n \subset I_{n+1}$, but this increasing sequence of ideals never ends. Therefore, $\mathbb{Z}[x_1, x_2, ...]$ is not Noetherian. $\square$

10 Problem 10

Notice that the product of generators is a generator for the product of ideals.

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

Then, these four elements generate the product of ideals. Notice that the difference of the second and the third generator is precisely $1 + \sqrt{-5}$, therefore the ideal $1 + \sqrt{-5}$ is contained in the product ideal.

To see the reverse containment, notice that $1 + \sqrt{-5}$ divides all the generators. It divides the second and third generators trivially, and the first and fourth using its conjugate.