Math 210B: Homework #3

Due on February 2, 2023

Professor Alexander Merkurjev

Nakul Khambhati

Problem 1

We are asked to show that $\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2}, a, b \in \mathbb{Z}\right\}$ is Euclidean. We claim that $\phi(a+b\sqrt{2}) = |a^2 - 2b^2|$ is a Euclidean function for this ring. Let $\alpha = a_1 + a_2\sqrt{2}, \beta = b_1 + b_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. We need to show that we can divide with remainder using this formula. In other words, we can write $\alpha = \gamma\beta + \delta$ for some $\gamma, \delta \in \mathbb{Z}[\sqrt{2}]$ with $\phi(\delta) < \phi(\beta)$. Note that this division is always possible in $\mathbb{Q}[\sqrt{2}]$ as $\dfrac{(a_1b_1 - 2a_2b_2) + (b_1a_2 - a_1b_2)\sqrt{2}}{b_1^2 - 2b_2^2}$ which we can write as $c_1 + c_2\sqrt{2}$ where c_1, c_2 can be read off the previous equation. In general, $c_1, c_2 \in \mathbb{Q}$. However, we can pick the nearest integers $q_1, q_2 \in \mathbb{Z}$ such that $|c_1 - q_1| \leq \frac{1}{2}$ and $|c_2 - q_2| \leq \frac{1}{2}$. Set $\gamma = q_1 + q_2\sqrt{2}$. Next, set $\theta = \frac{\alpha}{\beta} - \gamma$ so that $\theta\beta = \alpha - \gamma\beta$. Then, setting $\delta = \theta\beta$ we have $\alpha = \gamma\beta + \delta$. It remains to show that $\phi(\delta) < \phi(\beta)$. So, it suffices to show that $\phi(\theta) < 1$. We can evaluate $\phi(\theta) \leq (c_1 - q_1)^2 + 2(c_2 - q_2)^2 \leq \frac{3}{4}$.

Problem 2

We already saw that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal. We now need to show some ideal in the ring that cannot be expressed as aR for any a. Recall that since it is a principal ideal, there is some Euclidean norm $N(r)$ on the ring. It can be checked that $N(z) = a^2 + 5b^2$ is a valid norm for $z = a + b\sqrt{5}$. Consider the ideal $I = \langle 3, 1 + \sqrt{-5}\rangle$. If the ideal is principal then $\exists z : I = \langle z\rangle$. Then by properties of N, we have that $N(z)|9$ and $N(z)|6$ so $N(z)|3$. In particular, $z = a + b\sqrt{-5}$ has $b = 0$ so $a = \pm 1$. But then $I = R$ which is a contradiction.

Problem 3

Here, we will use the fact that a prime p is the sum of two squares $\iff p = 1 \pmod 4$. Therefore, if $p = 3 \pmod 4$ then we cannot write it as the sum of squares. So, assume that p has a non-trivial factorization $p = mn$ so that $N(p) = p^2 = N(m)N(n)$. So, we must have $N(m) = p, N(n) = p$. In particular, we have written p as the sum of squares $a^2 + b^2$. This is a contradiction. So every factorization is trivial. So p is irreducible. In a PID, this means p is prime in $\mathbb{Z}[i]$. $2 = (1 - i)(1 + i)$ is not prime.

Problem 4

Assume that $p = 1 \pmod 4$. We then know that $x^2 = -1 \pmod{\text{p}}$ for some $x \in \mathbb{Z}/p\mathbb{Z}$. As a result, $p|(x^2 + 1)$ so $p|(x + i)(x - i)$. But since p does not divide either of the factors, p is not a prime in $\mathbb{Z}[i]$. Then, there is a nontrivial factorization $p = z_1z_2$. So then $z_1 \in \mathbb{Z}[i] \setminus \mathbb{Z}$ and $z_1 = a^2 + b^2$ for nonzero a, b. So, it is the sum of squares.

Problem 5

Consider the prime factorization of $10 = 2 \cdot 5 = (1 + i)(1 - i)(2 + i)(2 - i)$. The prime ideals in $\mathbb{Z}[i]$ are $(1 + i), (p)$ for $p = 3 \pmod 4$. So, $(i + 1), (2 + i), (2 - i)$ are prime ideals that contain 10. There are a total of 3.

Problem 6

Assume that p is a prime integer. Also assume that it has two distinct representations as sums of squares. Now, extend to $\mathbb{Z}[i]$. Assume that p is a prime gaussian integer. But then $p^2 = (a^2 + b^2)(c^2 + d^2)$ so that

Problem 6 continued on next page...

$N(z) = N(z_1)N(z_2)$ for some gaussian integers z_1, z_2. This shows that p is not prime in $\mathbb{Z}[i]$. However, p was taken as an integer so $p = 1 \pmod 4$. However, since we are given two distinct representations of squares that sum up to p we cannot have $p = 1 \pmod 4$. Therefore, we have a contradiction. So p is not a prime integer.

Problem 7

The proof follows from degree considerations. First, note that $R \subset R[x]$ and that units in $R[x]$ are precisely the units in R. Since $R[x]$ is a UFD, therefore a domain, even R is a domain. We know that for any $x \in R$, we have a unique factorization in $R[x]$ so we can write $x = p_1 \cdots p_n$ where each p_i is prime (i.e. irreducible) in $R[x]$. It suffices to show that each p_i is in R. If it's irreducible in $R[x]$ then it is definitely irreducible in the subring R. Use the fact that $\deg(fg) = \deg(f)\deg(g)$. Since $\deg(x) = 0$ we must have $\deg(p_i) = 0$ so each $p_i \in R$.

Problem 8

We are asked to show that $p = x^9 + y^9 + z^9$ is irreducible in $\mathbb{C}[x, y, z]$. We treat this ring as $\mathbb{C}[x, y][z]$. Consider $q = x + y$ which is irreducible therefore prime. It is clear that $q|(x^9 + y^9)$ and $q \nmid z^9$. Further, $q^2 \nmid (x^9 + y^9)$. This satisfies the Eisenstein criterion so p is irreducible in $\mathbb{C}[x, y, z]$.

Problem 9

Let $f, g \in R[x]$ such that $C(g) = R$ and $f = gh$ for some $h \in F[x]$. First note that we can multiply h by some $a \in R$ to get $ah \in R[x]$. Let's denote $C(ah) = bR$. Then, $af = g(ah)$. So, $a(C(f)) = bR$. Then, $a|b$ so that $b = ac$ for some $c \in R$. Then, $C(ah) = acR$ or ac divides every coefficient of ah. So c divides every coefficient of h and $h \in R[x]$.

Problem 10

In class we proved that if R is a UFD, then $R[x]$ is a UFD. Since $\mathbb{Q}$ is a field so a PID, it is clearly a UFD. Therefore, by induction, each $\mathbb{Q}[x_1, \ldots, x_n]$ is a UFD, so even $\mathbb{Q}[x_1, x_2, \ldots]$ is a UFD. However, this ring is clearly not finitely generated since $(1, x_1, x_2, \ldots)$ is the smallest generating set in the ring. Therefore, it is not Noetherian.