April 17, 2021

18.702 Comments on Problem Set 7

1. Chapter 13, Exercise 7.3. (*some norms with* $d = -26$)

The integers in $\mathbb{Z}[\delta]$ are $a + b\delta$, with $a, b \in \mathbb{Z}$, and the norm of $a + b\delta$ is $a^2 + 26b^2$.
I guess the simplest thing is just to check. First, $5^6 = a^2$ with $a = 5^3$. It is the norm of $5^3 + 0\delta$.
For the others, we can note that $4^2 \cdot 26 = 416$. If an integer < 416 is the norm of $a + b\delta$, then b must be ≤ 4. Knowing this, there isn't too much work to be done. $75 = N(7 + \delta)$, $250 = N(4 + 3\delta)$, and 375 is not a norm.

2. Determine the ideal class group in the ring of integers $R = \mathbb{Z}[\delta]$ when $\delta^2 = d$, with **(a)** $d = -37$, and **(b)** $d = -41$.

Both -37 and -41 are congruent 3 modulo 4. So $\mu = 2\sqrt{|d|/3}$, and $\mu < 8$. The primes that need to be examined are $p = 2, 3, 5, 7$. We know that 2 splits, and that: $(2) = P^2$ for some prime ideal P.

The case $d = -37$: A prime p splits if and only if the polynomial $x^2 + 37$ has a root modulo p. It has no root modulo $p = 3, 5, 7$. So those primes remain prime and don't ontribute to the ideal class group. The class group is generated by the prime ideal P that divides 2. It is a cyclic group of order 2.

The case $d = -41$: Here p splits if $x^2 + 41$ has root modulo p. It does have a root modulo $p = 3, 5$, and 7. Those primes all split. Let's say that $(3) = \overline{Q}Q$, $(5) = \overline{S}S$, and $(7) = \overline{T}T$. The classes $\langle P \rangle \langle Q \rangle$, $\langle S \rangle$, and $laT\rangle$ generate the class group.
We compute some norms:

$N(2 + \delta) = 45 = 3^2 \cdot 5$. From this we can conclude that $\langle S \rangle = \langle Q \rangle^{\pm 2}$.

$N(3 + \delta) = 50 = 2 \cdot 5^2$. This implies that $\langle S \rangle^2 = \langle P \rangle$.
Putting these two rpelations together with $\langle P \rangle^2 = 1$ shows that $\langle Q \rangle^6 = 1$, and that we an eliminate

3. Chapter 13, Exercise 8.4. (*the cases of unique factorization*)

The case $d = -43$ was done in class (see the summaries for April 2 and 5, and $d = -163$ is in the text. The remaining cases are similar.

4. Chapter 14, Problem 1.4. (*Schur's Lemma*)

(a) A module is simple if it isn't the zero module and if it has no proper submodule. Let V be a simple module, and let v be a nonzero element of V. The map $R \longrightarrow V$ that sends an element a of R to av is a homomorphism, and since V is simple, it is surjective. Therefore V is isomporphic to R/K, where K is the kernel of the map (First Isomorphism Theorem). The Correspondence Theorem tell us that submodules of V correspond to submodules of R (i.e. to ideals of R) that contain the kernel. Since V is a simple module, there are no such ideals except K and R. The ideal K isn't the unit ideal R because v isn't zero. So it is a maximal ideal.

(b) Let $\varphi : S \longrightarrow S'$ be a homomorphism of simple modules. Then since S is simple, its kernel is either 0 or S, ad since S' is simple, its image is either o or S'.

5. Chapter 14, Problem 4.5. (*lattices in the complex plane*)

Let V be the set of linear combinations of the elements α, β, γ. In order for V to be a lattice, the first condition is that they must contain elements that are independent over $\mathbb{R}$, i.e., they must span $\mathbb{C}$ as a real vector space.

Next, if the elements are contained in a lattice, they are integer combinations of two vectors, and therefore they are linearly dependent over the rational numbers $\mathbb{Q}$. We can clear the denominator in a linear relation to obtain one, say $a\alpha+b\beta+c\gamma = 0$, with $a, b, c \in \mathbb{Z}$. Conversely, if there is such a relation, and if $c \neq 0$, then V is contained in the lattice spanned by α/c and β/c. A subgroup of a lattice is a discrete group, so if it contains two independent vectors, it is a lattice.

So, α, β, γ span a lattice if and only if they span $\mathbb{C}$ as real vector space, and are linearly dependent over the rational numbers $\mathbb{Q}$.