Math 430 Tom Tucker
NOTES FROM CLASS 08/25/21

Main object of study in this class will be rings like $\mathbb{Z}[i] \subset \mathbb{Q}[i]$. Let's start with an example, using the ring $\mathbb{Z}[\sqrt{-19}]$...

We will show that if the ring $\mathbb{Z}[\sqrt{-19}]$ had all the same properties that $\mathbb{Z}$ has, then the equation $x^2 + 19 = y^3$ would have no integer solutions x and y. Suppose we did have such an integer solution $x, y \in \mathbb{Z}$. Then we'd have $(x + \sqrt{-19})(x - \sqrt{-19}) = y^3$.

We can show that $(x+\sqrt{-19})$ and $(x-\sqrt{-19})$ have no common prime divisors (recall notion of divisor). Let's recall the idea of primality from the integers. An integer p is prime if $p \mid ab$ implies that $p \mid a$ or $p \mid b$. We can use this same notion in any ring R: we say that π is prime if $\pi \mid ab$ implies that $p \mid a$ or $p \mid b$. Suppose that π divided both $(x+\sqrt{-19})$ and $(x - \sqrt{-19})$. Then π divides the difference of the two which is $2\sqrt{-19}$. This would mean that π divides either 2 or $\sqrt{-19}$. This in turn would mean that either 2 or 19 divides $(x + \sqrt{-19})(x - \sqrt{-19})$, which means that 2 or 19 divides y. But this is impossible, since 19^3 cannot divide $x^2 + 19$, nor can 2^3 divide $x^2 + 1$. The latter follows from looking at the equation $x^2 + 19$ modulo 8.

Thus, $(x + \sqrt{-19})$ and $(x - \sqrt{-19})$ have no common prime factor. Thus, we see that if π divides x^2+19, then π^3 divides either $(x+\sqrt{-19})$ or $(x-\sqrt{-19})$, since π cannot divide both. This follows from factorizing the two numbers as we have assumed we can.

Hence, we see that $(x + \sqrt{-19})$ must be a perfect cube in $\mathbb{Z}[\sqrt{-19}]$ (note that $\mathbb{Z}[\sqrt{-19}]$ has no units except 1 and -1), so we can write

$$(u + v\sqrt{-19})^3 = x + \sqrt{-19}$$

so

$$x = u^3 - 57uv^2$$

and

$$1 = 3u^2v - 19v^3.$$

The latter equation gives $v(3u^2 - 19v^2) = 1$, so v is 1 or -1. If $v = 1$ we obtain $3u^2 - 19 = 1$, so $3u^2 = 20$. If $v = -1$, we obtain $3u^2 - 19 = -1$, so $3u^2 = 18$. Either way, there is no such integer u, so there was no solution to

$$x^2 + 19 = y^3.$$

But there is a solution

$$18^2 + 19 = 7^3.$$

So something is wrong. The ring $\mathbb{Z}[\sqrt{-19}]$ is different from $\mathbb{Z}$ in some way.

What went wrong? We don't have unique factorization, so the argument about ab being a perfect cube forcing a and b to be perfect cubes isn't correct.

We'll be working with rings R that are similar to $\mathbb{Z}[\sqrt{-19}]$.

- Is R a unique factorization domain?
- If not, how badly does it fail to be a unique factorization domain?

Definition 1.1. An element π of a ring A is said to be prime if $\pi \mid ab$ means $\pi \mid a$ or $\pi \mid b$.

Definition 1.2. A domain R is said to be a unique factorization domain if every $a \in R$ that is not a unit can be written as

$$a = \pi_1^{e_1} \cdots \pi_n^{e_n}$$

(where all of the π_i are prime)

Example 1.3. The integers $\mathbb{Z}$ are a unique factorization domain.

Let's start answering the first question. A partial answer is that the good subring B will be finitely generated as a module over $\mathbb{Z}$. This means that all of the elements in it will be *integral* over $\mathbb{Z}$.

For the rest of the class A and B are rings Recall that a monic equation over A is an equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

Definition 1.4. Let $A \subset B$. An element $b \in B$ is said to be integral over A if b satisfies an equation of the form

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0,$$

where the $a_i \in A$ (i.e., if it satisfies an integral equation over A).

The rings we work with will be subrings of K, where K is a number field (a finite extension of $\mathbb{Q}$). These rings will be integral over $\mathbb{Z}$.

It turns out that a key property for these rings is that they be *integrally closed* in their field of fractions. The ring $\mathbb{Z}[\sqrt{-19}]$ is not, it turns out, because $\frac{1+\sqrt{-19}}{2}$ is integral over $\mathbb{Z}$.

NOTE: ALL RINGS IN THIS CLASS ARE COMMUTATIVE WITH MULTIPLICATIVE IDENTITY 1 ($1 \cdot a = a$ for every $a \in A$, where A is the ring) AND ADDITIVE IDENTITY 0 ($0 + a = a$ for every $a \in A$ where A is the ring)

Definition 1.5. A ring R is called a principal ideal domain if for any ideal $I \subset R$ there is an element $a \in I$, such that $I = Ra$.

Later we'll see that for the rings we work with in this class, principal ideal domains and unique factorization domains are the same thing.

Proposition 1.6 (Easy)**.** *Let $A \subset B$. Then b is integral over $A \Leftrightarrow A[b]$ is finitely generated as an A-module.*

Proof. ($\Rightarrow$) Writing

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0,$$

we see that b^n is contained in the A-module generated by $\{1, b, \ldots, b^{n-1}\}$. Similarly, by induction on $r > 0$, we see that b^{n+r} is contained in the A-module generated by $\{1, b, \ldots, b^{n-1}\}$, since

$$b^{n+r} = -(a_{n-1}b^{n-1} + \cdots + a_1 b + a_0)b^r,$$

and is therefore contained in A-module generated by $\{1, b, \ldots, b^{n+(r-1)}\}$.

($\Leftarrow$) Let $\left\{\sum_{j=1}^{N_i} a_{ij}b^j\right\}_{i=1}^{S}$ generate $A[b]$. Then for M larger than the largest N_i, the element b^M can be written as A-linear combination of lower powers of b. This yields an integral polynomial over A satisfied by b. □

Definition 1.7. We say that $A \subset B$ is integral, or that B is integral over A if every $b \in B$ is integral over A.

Corollary 1.8. *If $A \subset B$ is integral and $B \subset C$ is integral, then $A \subset C$ is integral.*

Proof. Exercise. □