Math 531 Tom Tucker
NOTES FROM CLASS 9/1/04

Main object of study in this class will be rings like $\mathbb{Z}[i] \subset \mathbb{Q}[i]$. These rings are integral extensions (we'll define this ter later) of $\mathbb{Z}$. We will also work a bit with integral extensions of rings like $K[x]$, the ring of polynomials in x with coefficients in a field K. Let's start with an example, using the ring $\mathbb{Z}[\sqrt{-19}]$

asd asdfasdfa(

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 could write

$$(x + \sqrt{-19})(x - \sqrt{-19}) = y^3.$$

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 $p = uv$ implies that u or v is a unit. We can use this same notion in any ring R: we say that π is prime if $\pi = uv$ implies that u or v is a unit. 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, *weobtain*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? First of all, $\mathbb{Z}[\sqrt{-19}]$ is not the "right ring". I'll say what this means later. Moreover, even if it were, this "right ring" might not have all the same properties as $\mathbb{Z}$.
Let's do a quick outline of the questions we'll try to answer in this course

- Given a finite extension K of $\mathbb{Q}$, what is a good subring to work with, where "good" means most like $\mathbb{Z}$? Example: $\mathbb{Z}[i]$ in $\mathbb{Q}(i)$ is very much like $\mathbb{Z}$ (see problem set).

- What properties will this good subring have? Is it a principal ideal domain? What does the group of units look like? How do the primes from $\mathbb{Z}$ split up in this ring? Example: in $\mathbb{Z}[\sqrt{5}]$, $5 = \sqrt{5}\sqrt{5}$. What does 7 look like in this ring?

- What can we say about the units in the subring of K that we work with?

Example 1.1. Do $\mathbb{Z}[i]$.

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 an integral equation over A is an equation

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

Definition 1.2. 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).