Math 525 Class 14 September 27.

Homework will be postponed to Friday.

No quiz Friday.

* IMPORTANT *

Most problems in this textbook have solutions online somewhere.

It is OK to look up solutions.

By turning in a solution, even one obtained with the help of your friend "Google", you are representing that you understand what you have writtend, and that you could solve a similar problem on a test (time permitting)

Suggestion: think about the problem before looking it up! When you see the solution ask: what did I miss?

Recall that $\mathbb{Z}[\sqrt{-5}]$ is NOT a UFD.

$$3 \cdot 3 = 9 = (2+\sqrt{-5})(2-\sqrt{-5})$$

Claim: 3, $2+\sqrt{-5}$, and $2-\sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Proof: These elements have norm 9.

$$N(a+b\sqrt{-5}) = a^2+5b^2$$

Norm is multiplicative, so if $\alpha\beta = 2+\sqrt{-5}$

then $N(\alpha)N(\beta) = N(2+\sqrt{-5}) = 9$.

Thus either one of α, β has norm 1

or $N(\alpha) = N(\beta) = 3$.

But there are no elements of norm $a^2+5b^2 = 3$

Thus one of α, β has norm 1, so α or β is ± 1 and $2+\sqrt{-5}$ is irreducible.

The same argument applies to 3, $2-\sqrt{-5}$.

What is the $\gcd(3, 2+\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$

Note that $3 \nmid 2+\sqrt{-5}$ and vice versa.

3 and $2+\sqrt{-5}$ are irreducible, so any divisor is the same element (up to a unit).

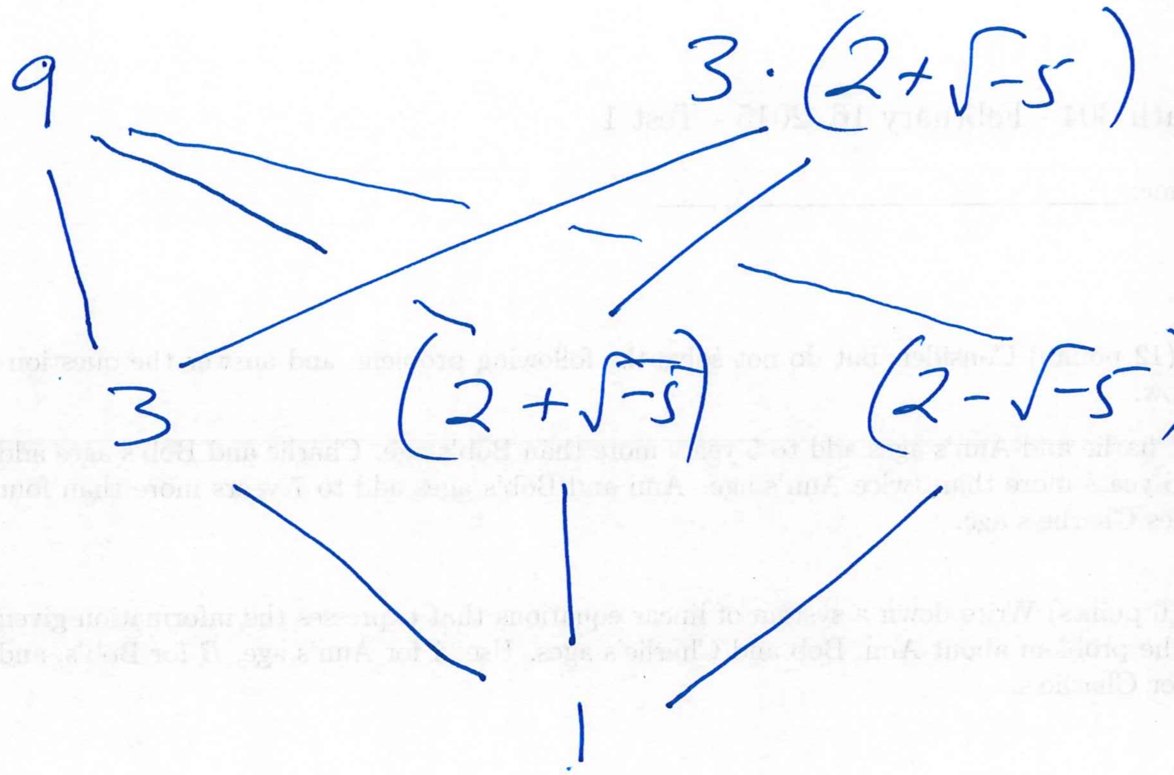
Thus $\gcd(3, 2+\sqrt{-5}) = 1$.

What is $\gcd(3^2, 3\cdot(2+\sqrt{-5}))$?

Note that there is a uniqueness requirement in the definition of gcd: the gcd d is required to divide a and b.

AND if $d' \mid a$, $d' \mid b$ we must have $d' \mid d = \gcd(a,b)$.

Let's draw a picture!



Note that $2+\sqrt{-5}$ is a common divisor:

$$(2+\sqrt{-5})(2-\sqrt{-5}) = 9$$

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

AND 3 is a common divisor:

$$3 \cdot 3 = 9 \qquad 3 \cdot (2+\sqrt{-5}) = 3 \cdot (2+\sqrt{-5}).$$

But there is no common divisor satisfying the uniqueness requirement.

$3 \nmid (2+\sqrt{-5})$ and vice versa

So neither can be the gcd.

In fact the GCD does not exist.

So the point of # 7 in 8.2 is that in a "Bezout Domain" by definition the gcd (a,b) is a linear combination $xa+yb$, and so gcds <u>do</u> exist.

So if you have $\frac{a}{b}$ you can factor out the gcd and get "lowest terms": no common factor.

But wait! In $\mathbb{Z}[\sqrt{-5}]$ we can do this anyway.

Consider, for example $\frac{9}{3(2+\sqrt{-5})}$

We can write $9 = 3\cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$

So $\frac{9}{3(2+\sqrt{-5})} = \frac{3}{2+\sqrt{-5}}$ AND $\frac{9}{3\cdot(2+\sqrt{-5})} = \frac{2-\sqrt{-5}}{3}$

Can we always do this?

No: Let $R = \mathbb{Z} + x\,\mathbb{Q}[x,y] + y\,\mathbb{Q}[x,y]$

R = polyns in $\mathbb{Q}[x,y]$ with integer constant term.

Now consider $\frac{x}{y}$

For any n we can write $n \cdot \left(\frac{1}{n}x\right) = x$.

So $\frac{n}{n} \cdot \frac{\frac{1}{n}x}{\frac{1}{n}y} = \frac{x}{y}$

and we can remove a factor of n from top and bottom for any n.

So $\frac{x}{y} = \frac{2}{2} \cdot \frac{\frac{1}{2}x}{\frac{1}{2}y} = \frac{2}{2} \cdot \frac{2}{2} \cdot \frac{\frac{1}{4}x}{\frac{1}{4}y}$ etc.

We can keep removing factors indefinitely

There is no such thing as lowest terms.

Why do I say "uniqueness requirement" in part (2)(ii) of defn of gcd p. 274?

Because if there were two gcds, d, $\tilde{d}$ then the definition implies $d \mid \tilde{d}$ and $\tilde{d} \mid d$, so they are the same up to a unit.

Example: in $\mathbb{Z}$ $\gcd(12, 9)$ can be 3 or -3.

Q: Why can't we have a simpler example than

$R = \mathbb{Z} + x\,\mathbb{Q}[x,y] + y\,\mathbb{Q}[x,y]$?

A: If factoring stops, we can get a representation which is not unique, but has lowest terms, as in $\frac{9}{3(2+\sqrt{-5})} = \frac{3}{2+\sqrt{-5}} = \frac{2-\sqrt{-5}}{3}$.

If it doesn't, the ring doesn't satisfy ACC, so must be "complicated".

In $\mathbb{H}$ how many solutions are there to

$$X^2 + I = 0 \ ?$$

In $M_{2\times 2}(\mathbb{R})$ how many soln's to $X^2 + I = 0$?

In $M_{2\times 2}(\mathbb{R})$: reflection in any line through the origin. is a linear trans with $X^2 = I$.

Rotation by 90° has $X^2 = -I$.

Infinitely many matrices with $X^2 = -I$.

In $\mathbb{H}$, let ~~[illegible]~~ $x, y, z \in \mathbb{R}^3$ with

$$x^2 + y^2 + z^2 = 1$$

Claim : $(xi + yj + zk)^2 = -1$.

infinitely many?