Math 525 Class 3 August 28

HW 2 (the first real HW) has been assigned.

No quiz Wed. Aug. 30th.

Quiz on 7.2 - 7.3 Friday Sep 2nd.

Grading: HW 20 Quiz 30

Midterm ~~X~~ 20 Final. 30.

Rings of integers in algebraic number fields

$\mathcal{O}_K$ in the notation of the text

Two important theorems:

(1) Finiteness of the Ideal Class Group.

(2) The group of units is finitely generated.

Gold standard of a mathematical concept being useful or important:

You can use X to prove a result that (a) makes no reference to X.

Math 525 — Quiz 1 – August 28

Name: Solutions

1. Complete the following definition of an ideal: An ideal I in a commutative ring R is a subset $I \subset R$ such that ...

I is an additive subgroup of R and if $r \in R$ and $a \in I$, then $ra \in I$.

2. Complete the following definition of an integral domain: A commutative ring R with 1 is called an *integral domain* if ...

it has no zero-divisors.

3. Is the matrix ring $M_2(\mathbb{R})$ a field? Why or why not?

No. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ has no inverse

4. Give the definition of the field norm $N\colon \mathbb{Q}[\sqrt{5}] \to \mathbb{Q}$, and find the norm of $2 + \sqrt{5}$.

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

$$N(2+\sqrt{5}) = (2+\sqrt{5})(2-\sqrt{5}) = -1.$$

and (b) could not otherwise be proved.

We could potentially weaken this to

(b') are hard/annoying to prove otherwise.

Rings of integers ~~are~~ in number fields can be used to prove results in number theory.
We therefore transfer our interest to studying such rings $\mathcal{O}_K$ directly since they meet the "Gold Standard".

Remarks on the Quaternions $\mathbb{H}$.

It turns out that the only non-commutative division algebra over $\mathbb{R}$ is $\mathbb{H}$.
Note that $\mathbb{C}$ is a division algebra over $\mathbb{R}$ but is commutative. The Octonions $\mathbb{O}$ are an 8-dimensional algebra over $\mathbb{R}$ which is not commutative but also not associative.

This is not obvious, and $\mathbb{R}$ plays a role in the truth of the statement.

Over $\mathbb{Q}$ we can construct ~~as~~ a ring from $\mathbb{Q}^4$.

$\mathbb{Q}1 + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$.

and declare $ij = -ji$ etc as in $\mathbb{H}$,

$$i^2 = -1 \quad j^2 = -1 \quad k^2 = -3.$$

This is not isomorphic to the same construction when $k^2 = -1$.

Why doesn't this work over $\mathbb{R}$?

There is a theory of "cyclic algebras" over a field.

More about $\mathbb{H}$: it comes with an involution

<u>extending complex</u> conjugation.

$$\overline{a + bi + cj + dk} = a - bi - cj - dk.$$

if $r, s \in \mathbb{H}$, $\overline{rs} = \bar{s} \cdot \bar{r}$.

Note that $\mathbb{H} \cong \mathbb{R}^4$ as vector spaces.

If $r, s, v \in \mathbb{H}$ think of $v \in \mathbb{R}^4$

We can construct. $r v \bar{s} \in \mathbb{H} \cong \mathbb{R}^4$.

This gives a mapping $\mathbb{H} \times \mathbb{H}^{op} \to M_4(\mathbb{R})$.

Notice that if we have
(r,s), $(r',s') \in \mathbb{H} \times \mathbb{H}^{op}$

then $(r,s)(r',s')\,v = (r,s)\cdot[r' v \bar{s}']$

$= r r' v (\bar{s}' \cdot \bar{s})$ reg.

$= r r' v \underset{(op)}{\overline{s s'}}$

$= r r' v\, \overline{s's}$

HW: Find a unit ~~[crossed out]~~ of infinite order in $\mathbb{Z}[\sqrt{7}]$.

Note $N: \mathbb{Z}[\sqrt{7}] \longrightarrow \mathbb{Z}$ is multiplicative.

So a unit must have norm ± 1.

(and vice versa).