CA LECTURE 21

SCRIBE: JEREMY BRADFORD

A one lecture digression into algberaic number theory (hobbled to a certain extent by a lack of Galois theory!)

Definition: a *Dedekind domain (DD)* is ID which is N'ian, integrally closed and has dimension one.

These are important in number theory.

Definition: a *number field* is a subfield of $\mathbb{C}$ which is FD when considered as a VS over $\mathbb{Q}$. Equivalent: $F = \mathbb{Q}(\alpha_1, \ldots \alpha_n)$ where the α_i are algebraic complex numbers.

The ring of integers $\mathfrak{o}_F$ is the set of $\beta \in F$ which are *algebraic integers*, that is are integral over $\mathbb{Z}$.

Examples: in $\mathbb{Q}(i)$ the integers are $\mathbb{Z}[i]$. But watch out, if $\alpha = \sqrt{5}$ then $(1+\alpha)/2$ is an integer in $\mathbb{Q}(\alpha)$.

Fact: $\mathfrak{o}_F$ is a DD.

Proof: Using more field theory than we have available, it can be shown that $\mathfrak{o}_F$ is a free abelian group whose rank is $n = dim_{\mathbb{Q}}(F)$. That is to say there is a so-called "integral basis" $\beta_1, \ldots \beta_n$ such that $\beta_i \in \mathfrak{o}_F$ and every element of $\mathfrak{o}_F$ is a unique $\mathbb{Z}$-linear combination.

Examples: $1, i$ for $F = \mathbb{Q}(i)$, $1, (1+\sqrt{5})/2$ for $\mathbb{Q}(\sqrt{5})$.

Since $\mathbb{Z}$ is Noetherian, $\mathfrak{o}_F$ is a N'ian $\mathbb{Z}$-module and hence is a N'ian ring.

To check integral closure we need to know the FOF. It is easy to see that if β is algebraic over $\mathbb{Q}$ then there is an integer n such that $n\beta$ is integral over $\mathbb{Z}$. It follows that every element of F has form β/n where $\beta \in \mathfrak{o}_F$ and $n \in \mathbb{Z}$, so F is the FOF. Integral closure is immediate.

Finally need to check dimension one. Let β be in $\mathfrak{o}_F$ and let $f \in \mathbb{Z}[x]$ be monic of minimal degree such that $f(\beta) = 0$. The constant term of f is nonzero so 0 is not among the roots. If $\beta_1 = \beta, \ldots \beta_k$ are the roots of f they are all integral over $\mathbb{Z}$ and $\beta_1 \ldots \beta_k \in \mathbb{Z}$ (after all $f = \prod_i (x - \beta_i)$). It follows that $\beta_2 \ldots \beta_k \in \mathfrak{o}_F$, so that the principal ideal $\beta\mathfrak{o}_F$ intersects $\mathbb{Z}$ in a nonzero ideal. In particular if P is a nonzero prime ideal of $\mathfrak{o}_F$ then $P \cap \mathbb{Z}$ is a nonzero prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$. Now $p\mathbb{Z}$ is maximal and $\mathfrak{o}_F$ is integral over $\mathbb{Z}$ so that P is maximal.

Next we recall that in a N'ian ID of dim one every ideal $I \neq 0, R$ is uniquely a product of primary ideals with distinct radicals. The extra hypothesis for DD's is integral closure, we see what this buys us.

Fact: in a DD every nonzero primary ideal is a power of a nonzero prime ideal.

Note: converse will be true since nonzero primes are maximal, and for P prime the radical of P^n is P.

Proof: Let Q be P-primary and consider the localisation R_P. Combining various old theorems we see that R is a N'ian local ID of dimension one, and is also integrally closed. So it is a DVR. The primary ideals of R_P are precisely the powers of the unique maximal ideal and are in bijection with the primary ideals of R contained in P; it follows easily that $Q = P^n$ for some n.

So we see that in DD's every ideal $I \neq 0, R$ is uniquely a product of prime ideals.

Five minutes of gossip about number fields and their rings of integers:

(1) $\mathfrak{o}_F$ is not always a PID but every ideal is generated by at most two elements.
(2) A *fractional ideal* is a fg $\mathfrak{o}_F$-submodule of F. Equivalently it is I/β where I is an ideal of $\mathfrak{o}_F$ and $\beta \neq 0$ is in $\mathfrak{o}_F$. They can be multiplied just like ideals.
(3) The nonzero frac ideals form a group under multiplication, with the principal frac ideals as a subgroup. The quotient is a finite group called the *ideal class group*.
(4) $\mathfrak{o}_F$ is a UFD iff it is a PID, that is the ideal class group is trivial.
(5) If I is a nonzero ideal of $\mathfrak{o}_F$ then $\mathfrak{o}_F/I$ is finite.
(6) Let p be a prime number and factorise $p\mathfrak{o}_F = P_1^{e_1} \dots P_g^{e_g}$, where the P_i are prime ideals of $\mathfrak{o}_F$. Easily $P_i \cap \mathbb{Z} = p\mathbb{Z}$, so that $\mathbb{Z}/p\mathbb{Z}$ is a subfield of the finite field $\mathfrak{o}_F/P_i$. If we let f_i be the dimension of $\mathfrak{o}_F/P_i$ over $\mathbb{Z}/p\mathbb{Z}$ then $dim_{\mathbb{Q}}(F) = \sum_{i=1}^g e_i f_i$.

Now for something completely different (or maybe I mean no one expects the Spanish Inquisition).

We define rather general notions of *diagram* and *limit*.

Let $\mathbb{I}$ and $\mathbb{C}$ be categories. Then an $\mathbb{I}$-*indexed diagram* in $\mathbb{C}$ is just a functor from $\mathbb{I}$ to $\mathbb{C}$.

Example: if we take a category with objects $0, 1, 2$ where the arrows are ij from i to j when $i \leq j$ then the diagrams indexed by this are the familar commutative triangles.

A *cone over* F consists of an object c of $\mathbb{C}$ and a family $f_a : c \to F(a)$ of morphisms of $\mathbb{C}$, for a running through the objects of $\mathbb{I}$, subject to the following commutativity requirements: for all objects a and b and morphism $h : a \to b$ of $\mathbb{I}$, we have $F(h) \circ f_a = f_b$.

Now we make the class of cones over a fixed F into a category in the usual way. To be explicit if c_1 with f_a^1 and c_2 with f_a^2 are two cones over F then a morphism between them is a morphism $g : c_1 \to c_2$ such that $f_a^2 \circ g = f_a^1$ for all a.

Defn: a *limit* for the diagram F is a final object in the category of cones over F.

Remark: this is a generalisation of the notion of product. If we let $\mathbb{I}$ be the category with two objects and no morphisms between them then the diagrams are just ordered pairs of objects. The limits of the diagram c, d are exactly the products.