Math 122 – lecture notes, 12 December 2003

HW for Monday

Exercises 11.8.1, 11.8.3, 11.9.8, 11.9.10

Read §11.10

§I Clarification of some definitions and results

① "prime element" and "irreducible element" are not synonyms

prime elt. p is not a unit and $p|ab \Rightarrow p|a$ or $p|b$

· irreducible elt. r is not a unit and $r=ab \Rightarrow a$ is a unit or b is a unit

– Let R be a domain (no zero divisors)

prop: $p\neq 0$ prime $\Rightarrow p$ is irreducible

pf: $p=ab \Rightarrow p|ab \Rightarrow$ WLOG $p|a \Rightarrow cp=a \Rightarrow p=ab=pcb \Rightarrow p(1-cb)=0 \Rightarrow$

$\Rightarrow 1-cb=0 \Rightarrow b$ is a unit

WARNING: Converse is false for an arbitrary domain

ex: from last class $R=\mathbb{Z}[\sqrt{d}]$ where d is square-free, $d<-1$, $d\equiv 3 \bmod 4$

$2(\frac{1-d}{2})=(1-\sqrt{d})(1+\sqrt{d})$

· 2 is irreducible

· 2 is not prime: $2|(1-\sqrt{d})(1+\sqrt{d})$ but $2\nmid(1-\sqrt{d}), (1+\sqrt{d})$

② Special rings

		UFD	PID	ED	
$\{$all rings$\} \supset$	$\{$domains$\} \supset$	$\{$unique factorization domains$\} \supset$	$\{$principal ideal domains$\} \supset$	$\{$Euclidean domains$\} \supset$	$\{$fields$\}$
	no 0-div's.	"unique" up to reordering of factors and up to associates	$I=(d)$	δ: Euclidean norm $\forall a,b\neq 0$ $a=bq+r$ $r=0$ or $\delta(r)<\delta(b)$	
$\mathbb{Z}\times\mathbb{Z}$	$\mathbb{Z}[\sqrt{d}]$ $d<-1, d\equiv 3(4)$	$\mathbb{Z}[x]$ $(x,2)$ not principal	$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$	$\mathbb{Z}$	$\mathbb{R}$

③ addendum to ①

prop: if R is a UFD and $0\neq r\in R$, then r is irreducible $\Leftrightarrow$ prime

So in UFDs we sometimes interchange prime and irreducible

WARNING: don't misapply this!

§II Prime and maximal ideals

recall: a (prime) ideal $M\subsetneq R$ is maximal $\Leftrightarrow$ $M\subset I\subset R \Rightarrow I=M,R$

prop: M max'l ideal $\Leftrightarrow R/M$ is a field.

def: $P\subsetneq R$ is called a prime ideal if $ab\in P \Rightarrow a\in P$ or $b\in P$

§II Prime and max'l ideals

prop: p is a prime element $\Leftrightarrow$ (p) is a prime ideal

pf: $p \mid x \Leftrightarrow x \in (p)$ $[p \mid ab \Rightarrow p \mid a \text{ or } p \mid b] \Leftrightarrow [ab \in (p) \Rightarrow a \in (p) \text{ or } b \in (p)]$

WARNING: P prime $\not\Rightarrow$ $P = (p)$ for some prime elt. p

ex: $\mathbb{Z}[x,y]/(x,y) \cong \mathbb{Z}$

prime, but not principal

prop: P prime $\Leftrightarrow$ R/P is a domain

pf: $(\Rightarrow)$ $xy = 0$ in R/P

$\tilde{x}\ \tilde{y} \in R$ $\tilde{x}\tilde{y} \in P \Rightarrow \tilde{x} \in P$ or $\tilde{y} \in P \Rightarrow x = 0$ or $y = 0$

$(\Leftarrow)$ identical.

Cor: M max'l $\Rightarrow$ M prime

pf: R/M field $\Rightarrow$ R/M domain

Cor: R is a domain $\Leftrightarrow$ (0) is prime

pf: $R = R/(0)$

§III Dedekind domains

- multiplication of ideals

  $I, J \in R \Rightarrow$ define $IJ = \{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J \}$

  - $(a)(b) = (ab)$ in the case of principal ideals

- another type of special ring

def: let R be a domain with a field of fractions $K \neq R$. We say R is a Dedekind domain if, for all ideals $I \subset R$, $\exists$ another ideal $J \subset R$ s.t. $IJ = (r)$ is principal (assume $J \neq (0)$).

ex: $K = \mathbb{Q}(\sqrt{d})$, d is a square-free integer. Then $\mathcal{O}_K$, the ring of all alg. integers in K, is $\left\{ \begin{matrix} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \ (4) \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \ (4) \end{matrix} \right\}$. $\mathcal{O}_K$ is a Dedekind domain by

Artin, prop. 10.8.10: If I is an ideal of $\mathcal{O}_K$, then $I' = \{\alpha' = a - b\sqrt{d} \mid \alpha = a + b\sqrt{d} \in I\}$ is an ideal satisfying $II' = (n)$ for some $n \in \mathbb{Z}$.

rmk: this generalizes to fields $K \supset \mathbb{Q}$ of finite dimension over $\mathbb{Q}$:

thm: $\mathcal{O}_K$ is a Dedekind domain for such fields K.

- structure of ideals in a Dedekind domain

thm: let R be a Dedekind domain, $I \subset R$, $I \neq (0)$. Then I can be written uniquely (up to reordering) as $I = P_1 \cdots P_k$, where the P_i are nonzero prime ideals

§III Dedekind domains

- This gives a way of salvaging unique factorization

ex: in $\mathbb{Z}[\sqrt{-5}]$ $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, but $(6) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})\cdot(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$

is a unique factorization into prime ideals

§IV Class groups

thm: R is a PID $\Leftrightarrow$ R is a UFD and a Dedekind domain

rmk: forward direction is easy, reverse direction relies on the fact that any ideal in a Dedekind domain is generated by at most 2 elements.

new idea: "class groups" measures how far away a Dedekind domain is from being a PID.

- to define the class group of a Dedekind domain R, define an equivalence relation on ideals $I \sim J \Leftrightarrow \exists$ nonzero $r, s \in R$ s.t. $rI = sJ$. Let $\langle I \rangle$ denote the equivalence class or "ideal class" of I. Let $\mathcal{Cl}(R)$ = set of ideal classes $= \{\langle I \rangle, (0) \neq I \underset{\text{ideal}}{\subset} R\}$

prop: $\langle I \rangle \cdot \langle J \rangle = \langle IJ \rangle$ gives a well-defined group structure on $\mathcal{Cl}(R)$

Prop: If R is a Dedekind domain, then R is a PID $\Leftrightarrow$ $\mathcal{Cl}(R)$ is the trivial group

pf: $(\Rightarrow)$ $I = (a)$, $J = (b) \Rightarrow bI = aJ \Rightarrow I \sim J$

$(\Leftarrow)$ similarly easy

ex: $\mathcal{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}) = \{\langle 1 \rangle, \langle (2, 1+\sqrt{-5}) \rangle\} \cong \mathbb{Z}/2\mathbb{Z}$

- to calculate $\mathcal{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})})$ $d<0$, see §11.10