LECTURE 8 : FIELD OF FRACTIONS & CHINESE REMAINDER Th^{m}

The proof is very much like we did in LECTURE 7,

Th^{m} (15) (§7.5, p 261, DUMMIT & FOOTE)

Let R be a commutative ring. Let D be a nonempty subset of R which does not contain zero and does not contain any zero divisors and if $x, y \in D$ then $xy \in D$ (closed under multiplication). Then $\exists$ commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. Furthermore, the ring Q has the properties

(1.) every element of Q has form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$ then Q is a field

(2.) The ring Q is the "smallest" ring containing R in which all the elements of D become units, in the following sense: Let S be any commutative ring with identity and let $\varphi : R \longrightarrow S$ be any injective ring homomorphism such that $\varphi(d) \in S^{\times}$ for every $d \in D$. Then $\exists$ an injective homomorphism $\Phi : Q \longrightarrow S$ such that $\Phi|_R = \varphi$.

(any ring containing isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q)

Remark: in §15.4 D&F show an amped-up version of this construction where D can contain zero divisors it is known as $D^{-1}R$ the ring of fractions of R with respect to D a.k.a the LOCALIZATION OF R AT D

If we form the field of fractions for an integral domain then this produces a field naturally containing the given integral domain

$\boxed{E1}$ $R = \mathbb{Z}$, $D = \mathbb{Z} - \{0\}$ then

$$Q = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0 \right\} = \mathbb{Q}$$

$\boxed{E2}$ Let R be an integral domain then polynomials $R[x]$ is an integral domain and we know $(R[x])^\times = R^\times$, only nonzero constants are units. Then the field of fractions

$$\underbrace{Q = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in R[x],\ g(x) \neq 0 \right\}}$$

naturally identified with rational functions in x over R which we denote $R(x)$.
Every $\frac{f(x)}{g(x)} \neq 0$ has $\left(\frac{f(x)}{g(x)}\right)^{-1} = \frac{g(x)}{f(x)}$.

$\boxed{E3}$ Consider $R = 2\mathbb{Z}$ forms a ring without multiplicative identity. Using $D = 2\mathbb{Z} - \{0\}$ we find the field of fractions is:

$$\begin{aligned} Q &= \left\{ \frac{2a}{2b} \;\middle|\; a, b \in \mathbb{Z} \text{ with } b \neq 0 \right\} \\ &= \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0 \right\} \\ &= \mathbb{Q} \end{aligned}$$

Def^{n}/ The ideals A and B of a commutative ring R with identity $1 \neq 0$ are said to be <u>comaximal</u> if $A + B = R$

Recall we defined $AB = \{ \sum_{i=1}^{n} a_i b_i \mid a_i \in A, b_i \in B, n \in \mathbb{N} \}$ and also for principal ideals $A = (a)$ and $B = (b)$ we can verify $AB = (ab)$. Furthermore, for ideals $A_1, A_2, \dots, A_k$ the product ideal $A_1 A_2 \cdots A_k$ is once more defined by finite sums of products of form $a_1 a_2 \cdots a_k$ where $a_1 \in A_1$, $a_2 \in A_2, \dots, a_k \in A_k$. We can demonstrate if $A_j = (a_j)$ $\forall j = 1, 2, \dots, k$ then $A_1 A_2 \cdots A_k = (a_1 a_2 \cdots a_k)$.

$\boxed{E4}$ given $m, n \in \mathbb{N}$ with $\gcd(m,n) = 1$ we know by Bezout $\exists\, x, y \in \mathbb{Z}$ for which $mx + ny = 1$ thus $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ since $(m) = m\mathbb{Z}$ and $(n) = n\mathbb{Z}$ have $1 \in (m) + (n) \Rightarrow (m) + (n) = \mathbb{Z}$.

Thus $m\mathbb{Z}$ and $n\mathbb{Z}$ are <u>comaximal</u>

$\boxed{E5}$ $3\mathbb{Z}$ and $10\mathbb{Z}$ are comaximal $3\mathbb{Z} + 10\mathbb{Z} = \mathbb{Z}$.
and $10\mathbb{Z} = (10) = (2 \cdot 5) = (2)(5) = (2\mathbb{Z})(5\mathbb{Z})$

$\boxed{E6}$ $(1+x) = I$ and $(1-x) = J$ have that for commutative ring R containing $\frac{1}{2}$,
$\frac{1}{2}(1+x) + \frac{1}{2}(1-x) = 1 \in I + J$ $\therefore$ $I + J = R[x]$

Th^m/ (Chinese Remainder Theorem)

Let R be commutative ring with $1 \neq 0$ and suppose $A_1, A_2, \dots, A_k$ are ideals in R. Then the map $\varphi : R \longrightarrow R/A_1 \times R/A_2 \times \dots \times R/A_k$ defined by

$$\varphi(r) = (r + A_1, r + A_2, \dots, r + A_k)$$

is a ring homomorphism with $\ker\varphi = A_1 \cap A_2 \cap \dots \cap A_k$. Furthermore, if $A_i + A_j = R$ for all $i \neq j$ where $1 \leq i, j \leq k$ then φ is <u>surjective</u> and $A_1 \cap A_2 \cap \dots \cap A_k = A_1 A_2 \cdots A_k$ so,

$$\frac{R}{(A_1 A_2 \cdots A_k)} = \frac{R}{A_1 \cap A_2 \cap \dots \cap A_k} \cong \frac{R}{A_1} \times \frac{R}{A_2} \times \dots \times \frac{R}{A_k}$$

<u>Proof</u>: Notice $A_1, \dots, A_n$ ideals $\Rightarrow$ quotient rings R/A_j have quotient maps $\pi_j : R \to R/A_j$ given by

$$\pi_j(r) = r + A_j \quad \text{and} \quad \pi_j(rs) = \pi_j(r)\pi_j(s)$$

and $\pi_j(r+s) = \pi_j(r) + \pi_j(s)$ follow from

$$(r + A_j)(s + A_j) = rs + A_j \quad \text{and} \quad (r + A_j) + (s + A_j) = r + s + A_j.$$

Notice $\varphi = (\pi_1, \pi_2, \dots, \pi_k)$ thus φ is a ring homomorphism since all its component functions are ring homomorphisms. I'll show multiplication explicitly and leave addition to the reader,

$$\begin{aligned}
\varphi(r)\varphi(s) &= (\pi_1(r), \dots, \pi_k(r))(\pi_1(s), \dots, \pi_k(s)) \\
&= (\pi_1(r)\pi_1(s), \dots, \pi_k(r)\pi_k(s)) \\
&= (\pi_1(rs), \dots, \pi_k(rs)) \\
&= \varphi(rs)
\end{aligned}$$

Proof continued: ZERO

$r \in \ker\varphi \iff \varphi(r) = (r+A_1, r+A_2, \ldots, r+A_k) = (A_1, A_2, \ldots, A_k)$

$\iff r+A_1 = A_1, \; r+A_2 = A_2, \ldots, r+A_k = A_k$

$\iff r \in A_1, \; r \in A_2, \ldots, r \in A_k$

$\iff r \in A_1 \cap A_2 \cap \cdots \cap A_k$

Thus $\ker\varphi = A_1 \cap A_2 \cap \cdots \cap A_k$. Now we move on to the interesting and possibly nontrivial part, suppose A_i, A_j are comaximal whenever $1 \le i,j \le k$ and $i \ne j$. Hence $A_i + A_j = R$ for $i \ne j$ with $1 \le i,j \le k$.

We examine the proof for $A_1 = A$, $A_2 = B$ then proceed by induction.

Suppose A, B ideals with $A+B = R$. Consider $\varphi : R \longrightarrow (R/A) \times (R/B)$ given by $\varphi(r) = (r+A, r+B)$.

We need to show φ is surjective and $A \cap B = AB$, we've already shown φ is ring homomorphism. Since $A+B = R$, $\exists\, x \in A$, $y \in B$ for which $x+y = 1$ thus $1-x = y \in B$ and $1-y = x \in A$

Therefore,

$$\varphi(x) = (x+A, x+B) = (A, 1-y+B) = (0,1)$$

$$\varphi(y) = (y+A, y+B) = (1-x+A, B) = (1,0)$$

Now we can demonstrate surjectivity let $(r_1+A, r_2+B) \in (R/A) \times (R/B)$ then,

$$\begin{aligned}
\varphi(r_2x + r_1y) &= \varphi(r_2)\varphi(x) + \varphi(r_1)\varphi(y) \\
&= (r_2+A, r_2+B)(0,1) + (r_1+A, r_1+B)(1,0) \\
&= (0, r_2+B) + (r_1+A, 0) \\
&= (r_1+A, r_2+B).
\end{aligned}$$

Thus φ surjective.

Proof continued continued:

Observe $AB \subseteq A \cap B$. To see why this is true let $\tilde{x} = \sum_{i=1}^{n} a_i b_i \in AB$ where $a_i \in A$, $b_i \in B$ for $i = 1, 2, \dots, n$. Then $a_i b_i \in A$ and $a_i b_i \in B$ since A, B are ideals and also $\sum_{i=1}^{n} a_i b_i \in A$ and $\sum_{i=1}^{n} a_i b_i \in B$ since A, B are subrings. Hence $\tilde{x} \in A$ and $\tilde{x} \in B$ and we find $\tilde{x} \in A \cap B$ $\therefore$ $AB \subseteq A \cap B$.

Conversely, to see $A \cap B \subseteq AB$ we study $x \in A \cap B$ $c \in A \cap B$ and note $c = c \cdot 1 = c(x+y) = cx + cy \in AB$ hence $A \cap B \subseteq AB$ and we conclude $\underline{AB = A \cap B}$.

$$\underbrace{R/\ker\varphi = R/A \cap B = R/AB \cong R/A \times R/B}_{1^{st} \text{ isomorphism Th}^m \text{ for rings}}$$

Let's examine how induction completes the proof. Suppose Th^m holds for $(k-1)$-comaximal ideals and consider $A = A_1$, $B = A_2 \cdots A_k$. We need to show A & B are comaximal. We're given $\exists\, x_i \in A_1$ and $y_i \in A_i$ s.t. $x_i + y_i = 1$ for $i = 2, \dots, k$. Then $x_i + y_i + A_1 = y_i + A_1$ since $x_i \in A_1$ for $i = 2, \dots, k$.

Thus $1 = (x_2 + y_2)(x_3 + y_3) \cdots (x_k + y_k) \in A_1 + (A_2 A_3 \cdots A_k)$

Hence
$$\frac{R}{\ker\varphi} = \frac{R}{A_1(A_2 \cdots A_k)} \cong \frac{R}{A_1} \times \frac{R}{A_2 \cdots A_k} \underset{\uparrow \text{ induction hypothesis}}{\cong} \frac{R}{A_1} \times \frac{R}{A_2} \times \cdots \times \frac{R}{A_k}. //$$

Corollary: Given $\gcd(m,n) = 1$ for $m,n \in \mathbb{N}$ we find $\left(\mathbb{Z}/mn\mathbb{Z}\right)^\times \cong \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$

Moreover, for $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (prime power factorization of n)

$$\mathbb{Z}/n\mathbb{Z} \cong \left(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}\right) \times \left(\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}\right)$$

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$$

and,

$$\left(\mathbb{Z}_n\right)^\times \cong \left(\mathbb{Z}_{p_1^{\alpha_1}}\right)^\times \times \left(\mathbb{Z}_{p_2^{\alpha_2}}\right)^\times \times \cdots \times \left(\mathbb{Z}_{p_k^{\alpha_n}}\right)^\times$$

Recall $|\mathbb{Z}_n^\times| = \varphi(n)$ (Euler's φ function)

we find $\boxed{\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k})}$

$\boxed{E7}$ For odd prime p have $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ for $\alpha \geq 1$ for instance, $\varphi(5) = 4$, $\varphi(25) = 25 - 5 = 20$, $\varphi(125) = 100$.

$\boxed{E8}$ $\varphi(100) = \varphi(25)\varphi(4)$

$= (20)(2)$ since $\mathbb{Z}_4^\times = \{1, 3\}$.

$= \underline{40}$.

$\boxed{E9}$ $\varphi(67) = 66$.