Algebraic Theory I

Thomas Fleming

November 14, 2021

Contents

«««< HEAD «««< HEAD

Lecture 32

Sun 14 Nov 2021 15:09

=======

Lecture 32

Wed 10 Nov 2021 17:32

»»»> fbddf3e930553556ea514c68e105d294dc597cc6

Lecture 31: Noetherian Rings

Fri 05 Nov 2021 11:34

1 Noetherian Rings

Recall. A commutative ring is noetherian if it satisfies the ascending chain condition on ideals. We claimed this to be equivalent to the property that all ideals are finitely generated.

Proof. First, we assume R to be noetherian. Suppose there is an ideal I which is not finitely generated. Then, let $x_1 \in I$ be a nonzero element of I. Hence, we have $(0) \subset (x_1)$ with $(x_1) \neq I$ by assumption. Moreover, there is an $x_2 \neq x_1$ which is also nonzero such that $(0) \subset (x_1) \subset (x_1, x_2)$ and $(x_1, x_2) \neq I$ by assumption. Recursing, we see there are $x_1, x_2, \ldots \in I$ such that $(x_1, x_2, \ldots, x_n) \subset (x_1, x_2, \ldots, x_n, x_{n+1}) \subset I$ for all n. Hence, letting $I_n = (x_1, \ldots, x_n)$ we obtain an infinite strictly ascending chain of ideals $\lightning$. Hence, $I_n = I$ for some n, so I is finitely generated.

Now, assume all ideals are finitely generated. Suppose there is an infinite proper chain of ideals

$$I_0 \subset I_1 \subset \dots$$

with each containment being proper. Then, we see $\bigcup_{k \in N_0} I_k = I$ is an ideal. Moreover since I is finitely generated there are $y_1, y_2, \dots, y_n \in I$ such that $I = (x_1, x_2, \dots, x_n)$. Then, since $y_1, y_2, \dots, y_n \in \bigcup_{k \in N_0} I_k$, we see each one is in I_k for some k. Since each $I_k \subset I_{k+1}$, let I_m be an ideal containing all $y_1, y_2, \dots, y_n$. Then, we see $I \subset I_m$, but this is a contradiction as $I \neq I_m$ by the proper containment assumption and $I \nsubseteq I_m$ as I_m is within the union. $\lightning$. Hence, the chain cannot be strictly ascending. □

Proposition 1.1. Let R be a commutative ring. If R satisfies the ascending chain condition on all principal ideals, then every nonzero element in R has a factorization.

Proof. Let $x \in R$ be a nonzero, nonunit. If x is irreducible, $x = x$ is a factorization. Hence, we can assume $x = x_1 x_2$ with x_1, x_2 being nonzero, nonunits. Similarly, we see x_1, x_2 cannot both be irreducible else this would be a factorization. Hence define $x_1 = x_{11} x_{12}$ and $x_2 = x_{21} x_{22}$ with atleast 3 of $x_{11} x_{12} x_{21} x_{22}$ being non-units. Hence, $x_1 = x_{11} x_{12} x_{21} x_{22}$. Recursing n times yields

$$x = \prod_{i=1}^{2^n} x_i$$

with atleast 2^{n-1} elements being nonunits. If for some n, we find all x_i, $1 \leq i \leq 2^n$ to be irreducible (or units), then x has been factored. Hence, we may assume atleast one x_i to be not an irreducible for all n. Then, we see there must be a sequence k_i such that $(x) \subset (x_1) \subset (x_{k_1}) \subset (x_{k_2}) \subset \dots$ as each x_{k_i} splits into a product of elements which are not both irreducble or units. Moreover, each containment must be proper, so letting n grow yields $\lightning$, as such a chain will continue indefinitely unless all x_i are irreducble or units at some step. Hence we must have at some point all x_i to be irreducibles, hence x is factorable. □

Theorem 1.1. If R is a noetherian domain then R is a unique factorization domain if and only if all irreducible elements are prime.

Proof. Note, we have already shown all primes to be irreducible in an integral domain (hence noetherian domain) and we know UFD implies primes are irreducibles. Hence, only one implication remains to be shown, that all irreducible being prime implies UFD.
Since R is a noetherian domain, factorizations exist. Hence, we need only show these factorizations are unique. Suppose

$$\begin{aligned} x &= u x_1 x_2 \dots x_n \\ &= u' y_1 y_2 \dots y \end{aligned}$$

with u, u' being units and x_i, y_i being irreducibles for each i. We proceed by induction on $|\mathrm{Fac}(x)|$. If $|\mathrm{Fac}(x)| = 1$, then x is irreducible and the claim is obviously true. Of course the case $|\mathrm{Fac}(x)| = 0$ implies x a unit, hence not factorable, so the claim is vacuously true in this case.
Now, assuming the case $n-1$, if $|\mathrm{Fac}(x)| = n$ (as is the case in the original x), we see $x_1 \mid x$ with x_1 being irreducible, hence prime. Supposing the claim false, we see $x_1 \mid u'y_1y_2 \dots y_t$, so WLOG, $x_1 \mid y_1$ up to units. As y_1 is irreducible and divided by x_1 , we see $y_1 = x_1r_1$ with r_1 being a unit, hence $x_1 = y_1$ up to units. Repeating yields for each $1 \le i \le n$, $x_i = y_j$ for some $1 \le j \le t$ (up to permutation of the y_i's) up to units, hence

$$\begin{aligned} x &= ux_1x_2 \dots x_n \\ &= \hat{u}x_1x_2 \dots x_n y_s \dots y_t \text{ for a unit } \hat{u} \text{ and some } s \le t \ . \end{aligned}$$

This yields, $y_1y_2 \dots y_t = 1$ up to units, $\lightning$ as the y_i's were assumed nonunits. $\square$

=======

2 Ring Localization

Lecture 33: Localization of Rings

Wed 10 Nov 2021 17:33

Recall. Recall R denotes a commutative ing. If $S \subseteq R$ is a multiplicative subset, we see $x, y \in S$ implies $xy \in S$ and $0 \notin S$ but $1 \in S$.
Then, we define $S^{-1}R = \{X/s : x \in R, s \in S\}$. Then, we see $\frac{x_1}{s_1} = \frac{x_2}{s_2}$ if and only if there is an $s \in S$ so that $s(s_2x_1 - s_1x_2) = 0$. Of course, if R is an integral domain we see this iplies $s_2x_1 - s_1x_2 = 0$, the normal definition of fraction equality.

Now, we turn this set into a ring. We define $\frac{x_1}{s_1} \cdot \frac{x_2}{s_2} := \frac{x_1x_2}{s_1s_2}$ and $\frac{x_1}{s_2} + \frac{x_2}{s_2} = \frac{s_2x_1}{s_1s_2} + \frac{s_1x_2}{s_1s_2} = \frac{s_2x_1 + s_1x_2}{s_1s_2}$. Now, we need to show that $+, \cdot$ are well defined (meaining they do not vary for different representatives of a given equivalence class). This fact is easily checked by symbolic manipulation so we omit the proof. For the addition case suppose $\frac{x_1}{s_1} = \frac{x_1'}{s_1'}$ and similairly for $\frac{x_2}{s_2}$ then take the multiplicative representation of the fraction and multiply the $\frac{x_1}{s_1}$ representation by $-s_2s_2'ts$ and the $\frac{x_2}{s_2}$ representation by $-s_1s_1'st$ and by adding together these representations we see terms cancel and we obtain that addition is in fact well defined. Moreover, it is trivial to check that the ring axioms hold.

Definition 2.1 (Ring Localization)**.** We denote this new fraction ring $S^{-1}R$ to be the **localization of** R with additive identity $\frac{0}{1}$, multiplicative identity $\frac{1}{1}$ and $\frac{tx}{ts} = \frac{x}{s}$ for all $t \in S$.

Note that $s \in S$ is nonzero by definition, so $\frac{1}{s} \cdot \frac{s}{1} = \frac{1}{1} = 1_{S^{-1}R}$, so every element has an inverse.

Proposition 2.1. If R is a commutative ring with $S \subseteq R$ being a multplicative subset. Then the map

$$\begin{aligned} \pi : R &\longrightarrow S^{-1}R \\ x &\longmapsto \pi(x) = \frac{x}{1} \end{aligned}$$

is a ring homomorphism. Moreover, if S has no zero-divisors, then π is an injection.

Proof. If $x, y \in R$ then $\pi(x \pm y) = \frac{x \pm y}{1} = \frac{x}{1} \pm \frac{y}{1} = \pi(x) \pm \pi(y)$. Furthermore $\pi(1) = \frac{1}{1} = 1$.
Lastly, $\pi(xy) = \frac{xy}{1} = \frac{x}{1}\frac{y}{1} = \pi(x)\pi(y)$. Hence, π is a ring homomorphism. Now consider $\ker(\pi) = \left\{x \in R : \frac{x}{1} = \frac{0}{1}\right\}$. We see this implies an $s \in S$ so that $s(1x - 1 \cdot 0) = sx = 0$, hence s is a zero divisor if $x \neq 0$ $\lightning$. So, the kernel is trivial. □

Example. If R is a commutative ring and $P \subseteq R$ is a prime ideal, then $S := R \setminus P$ is a multiplicative set. Moreover, $0 \in P$ so $0 \notin S$ and $P \subset R$ is proper, so $1 \in S$.
If $x, y \in S$ with $xy \notin S$, then $xy \in P$ so $x \in P$ or $y \in P$ $\lightning$. So, S is closed under multiplication. Then the localization $S^{-1}R$ is often denoted R_P. This is the canonical example of localization which we will study more next class. ◇

The use of this construction is that it allows us to embed an integral domain R in a field $R_{(0)}$ called the **field of fractions**.

3 Chinese Remainder Theorem

Lecture 34: Chinese Remainder Theorem

Fri 12 Nov 2021 17:29

Theorem 3.1 (Classical Chinese Remainder Theorem)**.** If $m_1, \ldots, m_r$ are relatively prime integers, then for $a_1, \ldots, a_r$ we find an $x \in \mathbb{Z}$ so that $x \equiv a_i \mod m_i$ for each $1 \leq i \leq r$.

Theorem 3.2 (Generalized Chinese Remainder Theorem)**.** Let R be a commutative ring with $I_1, \ldots, I_n \subseteq R$ being ideals so that $I_i + I_j = R$ for all $i \neq j$. That is, the I_is are pairwise co-maximal. Then for any $x_1, \ldots, x_n \in R$ we find an $x \in R$ so that $x \equiv x_i \mod I_i$ for all $1 \leq i \leq n$.

Recall. $x \equiv x_i \mod I_i$ if $x - x_i \in I_i$.

Proof. If $n = 1$ this is trivial. Of course, $x = x$.
For the case $n = 2$ we have $I_1 + I_2 = R$, hence $1 \in R = I_1 + I_2$. Hence, $1 = a_1 + a_2$ with $a_1 \in I_1, a_2 \in I_2$. Then, let $x = x_1a_1 + x_2a_2$, and we see $a_1 + a_2 = 1$ but $a_1 \equiv 0 \mod I_1$ and likewise $a_2 \equiv 0 \mod I_2$, hence $a_1 \equiv 1$

mod I_2 and $a_2 \equiv 1 \mod I_1$. Hence,

$$\begin{aligned} x &= x_1 a_2 + x_2 a_1 \\ &\equiv x_1 a_2 \mod I_1 \\ &\equiv x_1 \mod I_1 \\ \text{and } x &\equiv x_2 a_1 \\ &\equiv x_2 \mod I_2. \end{aligned}$$

Hence, the claim holds for $n = 2$. Now, we induce on n.
Let $n \geq 3$ and suppose the case $n-1$ to be true. Then, we find Then, we see $I_1 + I_i = R$ for all $i \geq 2$ by hypothesis. Hence, $1 = a_i + b_i$ with $a_i \in I_1$, $b_i \in I_i$. Then, we find

$$1 = \underbrace{1 \cdot \ldots \cdot 1}_{n \text{ times}} = \prod_{i=1}^{n} (a_i + b_i) \in \prod_{i=1}^{n} (I_1 + I_i) \subseteq I_1 + \prod_{i=2}^{n} I_i.$$

Moreover, we know $I_1 + \prod_{i=2}^{n} I_i$ to be an ideal as the product and sum of ideals are still ideals.
Then applying the case $n = 2$, we find a $y \in R$ so that $y_1 \equiv 1 \mod I_1$ and $y_1 \equiv 0 \mod \prod_{i=2}^{n} I_i$. Repeating for each $1 \leq i \leq n$ yields a $y_j \in R$ so that $y_j \equiv 1 \mod I_j$ and $y_j \equiv 0 \mod \prod_{1 \leq i \leq n; i \neq j} I_i$. Now, define $x = \prod_{i=1}^{n} x_i y_i$. We see $y_j \in I_i$ for all $i \neq j$, hence $y_j x_j \equiv 0 \mod I_i$ for all $i \neq j$. Hence $x \equiv x_i y_i \equiv x_i \mod I_i$. □

Note that in the preceding proof $\prod I_i$ denotes the ideal product as defined in the homework. In the next theorem we will use this symbol for the cartesian product, so ideal products will be written without product notation when the context is not necessarily clear.

Corollary 1 (Alternative Statement of the Chinese Remainder Theorem)**.** Let R be a commutative ring with $I_1, \ldots, I_n \subseteq R$ being pairwise comaximal distinct ideals of R. Then the map

$$\begin{aligned} f : R &\longrightarrow \prod_{i=1}^{n} R/I_i \\ x &\longmapsto (x \mod I_i)_{1 \leq i \leq n} \end{aligned}$$

is a surjective ring homomorphism with kernel $\ker(f) = \bigcap_1^n I_i$. Specifically,

$$R/\left(\bigcap_{i=1}^{n} I_i\right) \simeq \prod_{i=1}^{n} (R/I_i).$$

Proof. It is easily confirmed that f is a ring homomorphism with the prescribed kernel. Hence, the only claim that remains to be shown is the surjectivity. For f to be surjective, we need to take an arbitrary congruence system $\hat{x} = (x_1 \mod I_1, x_2 \mod I_2, \ldots, x_n \mod I_n)$ in the codomain of f and find a solution $x \in R$ so that $x \equiv x_i \mod I_i$ for all $1 \leq i \leq n$ (that is $f(x) = \hat{x}$). We see the generalized remainder theorem yields such an x, so f is surjective. □

»»»> fbddf3e930553556ea514c68e105d294dc597cc6