Introduction to Rings and Modules

Lecture 22, Wednesday June 28 2023
Ari Feiglin

Recall the definition of Cauchy sequences, our definition for metric spaces or normed vector spaces also holds fields with an absolute value (as they are normed vector spaces), and it still holds for integral domains with absolute values as they are metric spaces. Also recall that the sum and product of two Cauchy sequences is also a Cauchy sequence, and thus given a ring R with an absolute value, we can define the ring of all Cauchy sequences over R. The additive identity of this new ring would be the sequence $\{0\}_{n\in\mathbb{N}}$ and the multiplicative identity would be $\{1\}_{n\in\mathbb{N}}$. Let us denote this new ring by $\mathcal{C}_R$.
Suppose R has an absolute value, then let us define $I\subseteq\mathcal{C}_R$ as the set of all sequences which converge to zero (recall if a sequence is convergent it is Cauchy). Now, if $\{a_n\}_{\mathbb{N}}\in I$ then let $\{b_n\}_{\mathbb{N}}\in\mathcal{C}_R$, since Cauchy sequences are bounded, suppose $|b_n|<M$ then $|a_nb_n|=|a_n||b_n|<M|a_n|$. Thus for any $\varepsilon>0$, there exists an N where for every $n>N$, $|a_n|<\frac{\varepsilon}{M}$ and so $|a_nb_n|<\varepsilon$ and so $\{a_nb_n\}_{\mathbb{N}}\in I$. And similarly the sum of two sequences in I also converge to zero, so too must their sum (in general the sum of two convergent sequences converges to the sum of their limits since $|a_n+b_n-a-b|\leq|a_n-a|+|b_n-b|$ by the triangle inequality), and so I is an ideal. But we claim even more than this.

Proposition 22.0.1:

If F is a field, then I (as defined above) is a maximal ideal of $\mathcal{C}_F$.

Proof:

Suppose that there exists an ideal such that $I\subset J$, then there exists some $\{a_n\}\in J\setminus I$ and so $I\subset(\{a_n\})+I\subseteq J$. Since we're claiming I is maximal, we must have that $(\{a_n\})+I$ is $\mathcal{C}_F$. So we will show that for every Cauchy sequence which does not converge to zero $\{a_n\}\in\mathcal{C}_R$, $I+(\{a_n\})=\mathcal{C}_F$.
Since a_n does not converge to zero, for large enough ns, $a_n\neq0$, so let us define the sequence $b_n=\frac{1}{a_n}$ when $a_n\neq0$, and zero otherwise. And since a_n does not converge to zero, there exists an $m>0$ such that eventually $|a_n|>m$ and so

$$|b_n-b_m|=\frac{|a_n-a_m|}{|a_n||a_m|}<\frac{1}{m^2}\cdot|a_n-a_m|$$

for large enough n and ms. So b_n is Cauchy. Notice that $\{a_n\}\cdot\{b_n\}$ is eventually 1_F, meaning that $1_{\mathcal{C}_F}-\{a_n\}\cdot\{b_n\}\in I$, or in other words $1_{\mathcal{C}_F}\in I+\mathcal{C}_F\{a_n\}$ as required. ■

Definition 22.0.2:

Thus ${}^{\mathcal{C}_F}\!/_I$ is a field, called the **completion** of F relative to $|\cdot|_F$. It is denoted $\overline{F}$.

We can embed F in $\overline{F}$ by mapping $a\in F$ to $\{a,a,\dots\}+I$.
In the case that $F=\mathbb{Q}$, if the absolute value is $|\cdot|_\infty$, then the completion of $\mathbb{Q}$ relative to this absolute value is the definition of the reals, $\mathbb{R}$ (we must first change our definitions of absolute values to restrict their values to being rational). If the absolute value is $|\cdot|_p$ then the completion is called $\mathbb{Q}_p$, the field of p-adic numbers.
Notice that if $\{a_n\}$ is a Cauchy sequence (in F with an absolute value of, say $|\cdot|^*$), then $|a_n|$ is a real Cauchy sequence since $\big||a|^*-|b|^*\big|\leq|a-b|^*$ by the triangle inequality. Thus since $\mathbb{R}$ is complete, we can define an absolute value on the completion of R by

$$|\{a_n\}|^*=\lim|a_n|^*$$

This is well-defined since if $\{a_n\}-\{b_n\}$ converges to zero, then $|a_n-b_n|^*$ converges to zero and so

$$|a_n|^*\leq|a_n-b_n|^*+|b_n|^*$$

meaning the limit of $|a_n|^*$ is less than that of $|b_n|^*$ and by symmetry the other direction is true as well, so the limits are the same. This is an absolute value since it obviously is non-negative, multiplicative, and satisfies the triangle inequality. And the limit of $|a_n|^*$ is zero if and only if a_n converges to zero, meaning $a_n\in I$ (the ideal of all zero-convergent sequences) so $\{a_n\}+I=0_{\mathcal{C}_F}$.
It is well-known that the completion of a metric space is complete. Thus $\overline{F}$ is complete.
If F is non-archimedean then so is its completion (ie. if the original absolute value satisfies the strong triangle inequality so does the new one on Cauchy sequences).

Proposition 22.0.3:

If $\{a_k\}_{k=0}^{\infty}$ is a sequence in $\mathbb{Q}_p$ then the series

$$\sum_{k=0}^{\infty} a_k$$

converges in $\mathbb{Q}_p$ if and only if a_k converges to zero in $\mathbb{Q}_p$.

Proof:

It is simple to see that if the series converges so too does the sequence. Now suppose $a_k \to 0$ in $\mathbb{Q}_p$, then for all $\varepsilon > 0$ there exists an N such that for every $n > N$, $|a_n|_p < \varepsilon$. Now since the p-adic absolute value, and therefore its extension to $\mathbb{Q}_p$, is non-archimedean, we have that for every $n > m > N$:

$$|(a_1 + \cdots + a_n) - (a_1 + \cdots + a_m)| = |a_{m+1} + \cdots + a_n| \leq \max\{|a_{m+1}|, \ldots, |a_n|\} < \varepsilon$$

thus the partial sums form a Cauchy sequence in $\mathbb{Q}_p$, which is complete and so the partial sums converge as required. ■

Proposition 22.0.4:

If F is a field with a non-archimedean absolute value, let $\mathcal{O} = \{a \in F \mid |a| \leq 1\}$, then $\mathcal{O}$ is a subring of F.

Proof:

If $a, b \in \mathcal{O}$ then $|ab| = |a||b| \leq 1$ so $ab \in \mathcal{O}$ and $|a - b| \leq \max\{|a|, |-b|\} \leq 1$ since F is non-archimedean, so $a - b \in \mathcal{O}$ meaning $\mathcal{O}$ is closed under multiplication and is an abelian group under addition. And since $|1| = 1$, $\mathcal{O}$ is a subring. ■

And if we define

$$I = \{a \in \mathcal{O} \mid |a| < 1\}$$

then I is an ideal of $\mathcal{O}$.

Definition 22.0.5:

Let R be a commutative ring, then R is a **localized ring** if it has only one maximal ideal (if it has a maximum ideal).

Proposition 22.0.6:

Let R be a commutative ring and $I \trianglelefteq R$. Then R is localized and I its maximal ideal if and only if for every $a \in R \setminus I$ is invertible.

Proof:

Suppose R is localized and there exists an $a \in R \setminus I$ which was not invertible, then (a) is a proper ideal of R and therefore contained within a maximal ideal M. But since R is local, $M = I$ and so $a \in (a) \subseteq M = I$ which is a contradiction. Now suppose that every $a \in R \setminus I$ is invertible. Then let $J \trianglelefteq R$ be a proper ideal and let $a \in J$ then a is not invertible and so $a \notin R \setminus I$ and so $a \in I$ as required. ■

Thus $\mathbb{Z}/p^n\mathbb{Z}$ is localized as $I = ([p])$ (where $[x]$ is the equivalence class of x, $[x] = x + p^n\mathbb{Z}$) satisfies the condition of the above proposition. This is since if $[a] \notin I$ then $p \nmid a$ and so $\gcd(a, p^n) = 1$ meaning a is invertible.
Now suppose F is a non-archimdean field, and $\mathcal{O}$ and I be defined as above. Let $a \in \mathcal{O} \setminus I$ then $|a| = 1$, and since $a \in F$ that means $a \neq 0$ so it is invertible in F. And since $\left|a^{-1}\right| = |a|^{-1} = 1^{-1} = 1$, we have that $a^{-1} \in \mathcal{O}$ as required.
If $F = \mathbb{Q}_p$ then $\mathcal{O}$ is denoted $\mathbb{Z}_p$ and is called the *p-adic integers*. $\mathbb{Z}_p$ has a simple structure as its only ideals are

$$(p) \supset (p^2) \supset (p^3) \supset \cdots \supset (0)$$

It turns out that

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$$

thus $\mathbb{Z}_p/p\mathbb{Z}_p$ is a field and so its ring of polynomials is a PID and therefore a UFD (and therefore a gcd domain as well).

Lemma 22.0.7:

Let $P \in \mathbb{Z}_p[x]$ and $\overline{P} = {}^{\mathbb{Z}_p}\!/_{p\mathbb{Z}_p}[x] \cong {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}[x]$ is its reduction, then if

$$\overline{P} = \overline{Q} \cdot \overline{R}$$

is a factorization into coprime polynomials, then there exists a factorization $P = QR$ where Q and R are polynomials in $\mathbb{Z}_p[x]$ whose reductions are $\overline{Q}$ and $\overline{R}$ respectively.

We will not prove this.
This is not true over $\mathbb{Z}$, for example $x^2 + 1 \in \mathbb{Z}[x]$ is irreducible, but modulo five: $x^2 + [1] = (x - [2])(x - [3])$.

Definition 22.0.8:

If R is a ring (not necessarily commutative), it is called **simple** if it has no two-sided ideals other than (0) and R.

Fields are therefore simple, and recall that ideals of $M_n(R)$ are of the form $M_n(I)$ where $I \trianglelefteq R$, so if F is a field then $M_n(F)$ is simple as well (in general $M_n(R)$ is simple for simple rings R).

Definition 22.0.9:

If R is a ring, an element $e \in R$ is **idempotent** if $e^2 = e$.

Obviously 0 and 1 are idempotent in every ring.

Proposition 22.0.10:

If R is a domain (no zero-divisors), then the only idempotent elements in it are 0 and 1.

This is trivial: suppose $a^2 = a$ then $a(a-1) = 0$ and so $a = 0$ or $a - 1 = 0$ meaning $a = 1$.

Proposition 22.0.11:

If $e \in R$ is idempotent then $eRe = \{eae \mid a \in R\}$ is a ring.

Proof:

eRe is a subrng of R since

$$eae - ebe = e(a-b)e \in eRe$$

and

$$(eae)(ebe) = eaebe \in eRe$$

and $e \in eRe$ is the unit since $e = e1e$ so $e \in eRe$ and

$$e(eae) = e^2ae = eae, \quad (eae)e = eae^2 = eae$$

■