Math 412: Rings and Modules

Taught by Jenia Tevelev
Scribed by Ben Burns

UMass Amherst

Spring 2022

Contents

1 Rings and Fields

Definition 1. A Ring R is a set with 2 binary operations $+$ and $\cdot$ that satisfy the following axioms

1. $(R, +)$ is an abelian group: associative, commutative, existence of identity and inverses
2. Multiplication is associative
3. $\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c$ (left distributive) and $(a + b) \cdot c = a \cdot c + b \cdot c$ (right distributive)

Definition 2. A subset S of a ring R is called a subring if S is a ring with respect to the binary operations of R

Definition 3. A ring R is commutative if multiplication is also commutative

Remark 4. $(R, \cdot)$ is almost never a ring since 0 (the general additive identity) is almost never invertible with respect to $\cdot$

Example 5 (Non-commutative rings)**.** $Mat_n(\mathbb{R})$ with generic element, addition, and multiplcation defined as
$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in Mat_n(\mathbb{R})$
$(a_{ij}) + (b_{ij}) = a_{ij} + b_{ij}$
$\begin{pmatrix} a_{i1} & \dots & a_{in} \end{pmatrix} \cdot \begin{pmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix} = \begin{pmatrix} a_{i1}b_{1j} + \ldots + ainb_{nj} \end{pmatrix}$

Example 6 (Rings of functions)**.** $F = \{f | f : \mathbb{R} \to \mathbb{R}\}$
$(f + g)(x) = f(x) + g(x)$
$(f \cdot g)(x) = f(x)g(x)$

Definition 7. R is a ring with unity 1 if $\forall a \in R : a \cdot 1 = 1 \cdot a$

Note that rings don't necessarily have unity. For example, $(2\mathbb{Z}, +, \cdot)$ has no unity, but satisfies all ring axioms

Remark 8. $(\mathbb{Z}_n, +)$ is cyclic abelian group with generator 1. 1 is also unity for modular multiplication

Definition 9 (Direct Product of Rings)**.** For R, S, rings, we define the direct product of R and S
$R \times S = \{(r, s) | r \in Rs \in S\}$.
$(r, s) + (r', s') = (r + r', s + s')$
$(r, s)(r', s') = (rr', ss')$

Definition 10. For rings R, S a function $\phi : R \to S$ is a homomorphism if $\forall a, b \in R$, $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$. An isomorphism is a bijective homomorphism.

2 Fermat's and Euler's Theorems

Definition 11. Define R as a ring with unit 1. $a \in R$ is called a unit if $ab = ba = 1$ for some $b \in R$.

For example, take $R = Mat_n(\mathbb{R})$. R's unity is the identity matrix Id.
$A \in R$ is a unit $\iff AB = BA = \text{Id}$ for some $B \in Mat_n(\mathbb{R})$
$\iff$ A is an invertible matrix
$\iff \det A \neq 0$

If $R = \mathbb{Z}_p$, p prime, $x \in \mathbb{Z}_p$ is a unit $\iff x \neq 0$

Exercise 12 (HW). $R^* = \{a \in R | a \text{ is a unit }\}$. R^* is a group w/ respect to multiplication

For example, $\mathbb{Z}_p^*$ is a group of order $p - 1$. In every finite group G, the order of every element divides the order of the group (Lagrange Corollary)
$a^n = 1$ if $n = order(G)$

Corollary 13 (Fermat's Little Theorem). $x \in \mathbb{Z}_p^* \implies x^{p-1} = 1 \in \mathbb{Z}_p^*$.

Equivalently, $x \in \mathbb{Z}, \gcd(x, p) = 1 \implies x^{p-1} \equiv 1 \pmod p$.

Equivalently, $x \in \mathbb{Z} \implies x^p \equiv x \pmod p$. If $\gcd(p, x) = 1$, multiply both sides of the result of Fermat's Little Theorem by p. Otherwise, $\gcd(p, x) > 1$, $x \nmid p$ since p prime, so $p|x \implies x \equiv 0 \pmod p$, therefore $x^p \equiv 0 \equiv x \pmod p$.

Example 14. Show that $n^{33} - n$ always divisible by 15 for all n.

We want to show that $n^{33} - n$ is divisible by both 3 and 5 individually, which will then imply it is divisible by 15.

If $3|n$, then $n^{33} - n$ is trivially divisible by n. Else, $\gcd(n, 3) = 1$ since 3 is prime, so by FLT,

$$\begin{aligned}
n^2 &\equiv 1 \pmod 3 \\
(n^2)^{16} &\equiv 1^{16} \pmod 3 \\
n^{32} &\equiv 1 \pmod 3 \\
n^{33} &\equiv n \pmod 3 \\
n^{33} - n &\equiv 0 \pmod 3
\end{aligned}$$

The proof is same for 5: if $5|n$, then it is trivial, else we apply FLT to say that $n^4 \equiv 1 \pmod 5$, raise both sides to the 8th power, multiply by n, and substract by n.

Example 15. For $R = \mathbb{Z}_n$, $x \in \mathbb{Z}_n$ is a unit $\iff \gcd(x, n) = 1$.

Definition 16. The order of $\mathbb{Z}_n^*$ is $\phi(n)$.

Here, $\phi(n)$ is the Euler totient function, or the number of integers up to n that are coprime to n. This goes with the preceeding example, since this will count exactly the number of elements $\in \mathbb{Z}_n$ such that $\gcd(x, n) = 1$, which are therefore exactly the number of units.

For p prime, $\phi(p) = p - 1$, since no $d \in \{1, 2, \ldots p - 1\}$ may divide p, since p is prime. $\phi(p^k) = p^k - p^{k-1}$ since the elements that are not coprime to p^k are $\{p, 2p, \ldots, p^{k-1}p\}$. There are p^{k-1} such values, so the remaining $p^k - p^{k-1}$ values are coprime to p^k.

Theorem 17. $n = rs$, r, s *coprime*, $\mathbb{Z} \cong \mathbb{Z}_r \times \mathbb{Z}_s$ *(as rings). Implies Chinese Remainder Theorem*

Theorem 18. R *and* S *are rings with unity 1* $\implies (R \times S)^* \cong R^* \times S^*$

$(a, b) \in R \times S$ is a unit $\iff (a, b) * (c, d) = (c, d) * (a, b) = (1, 1)$ unity in $R \times S$ for some (c, d)
$\iff ac = ca = 1$ and $bd = db = 1$
$\iff a \in R^*$ and $b \in S^*$
$\iff (a, b) \in R^* \times S^*$

Corollary 19. r, s *coprime*, $n = rs \implies \mathbb{Z}_n^* \cong \mathbb{Z}_r^* \times \mathbb{Z}_s^*$

Corollary 20. r, s *coprime* $\phi(n) = \phi(r)\phi(s)$ *(multiplicative function)*

If r, s are coprime, then the multiples of r and the multiples of s cannot intersect until rs. Therefore, the numbers coprime to rs will be products of numbers $1 \leqslant x \leqslant r$ coprime to r and $1 \leqslant y \leqslant s$ coprime to s, and we can use a combinatorial argument to say that there are $\phi(r)\phi(s)$ such pairs.

Corollary 21. *Write* $n = p_1^{k_1} \cdots p_r^{k_r}$. *Then* $\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) = (p_1^{k_1} - p^{k_1 - 1}) \cdots (p_r^{k_r} - p_r^{k_r - 1})$

This is simply leveraging the preceeding Corollary that $\phi(n)$ is multiplicative, and pairwise breaking up n into seperate $\phi(p_i^{k_i})$ terms.

Corollary 22 (Euler's Theorem)**.** $x \in \mathbb{Z}_n^* \implies x^{\phi(n)} = 1 \in Z$

Recall that $\phi(n)$ is the order of $\mathbb{Z}_n^*$. For $A = \mathtt{order}(x)$, by Corollary to Lagrange, $o|\phi(n)$, so $\exists n : An = \phi(n)$, and $n^{\phi(n)} = n^{An} = (n^A)^n = 1^n = 1 \in \mathbb{Z}_n^*$.

Theorem 23. $\mathbb{Z}_p^*$ *is a cyclic group*

The proof will come later. For now, we can use this to say Z_p^* has a generator or that Z_7^* has a generator

Example 24. Determine existence of solutions for, and determine solutions of an equation (congruence) $ax = b \in \mathbb{Z}_n$.

MAGMA: Solution(a, b, n) returns sequence of solutions if they exist, and -1 if no solution.

To determine $d := \gcd(a, n)$, $ax \equiv b \pmod{n} \implies d|b$. In other words, $ax + ny = b \implies ax + ny \equiv 0 \equiv b \pmod{d}$.

If $d \nmid b$ then there are no solutions. Else, $a = a'd, b = b'd, n = n'd$. $ax \equiv b \pmod{n}$, so $a'd \equiv b'd \pmod{n'd}$. Divide the equivalent Diophantine equation by d to obtain $a'x \equiv b' \pmod{n'}$. $\gcd(a', n') = 1$ (else $d < \gcd(a, n)$) so a is invertible in $Z_{n'}$. $1 \equiv a'c'$ in $\mathbb{Z}_{'}$

Multiply both sides of $a'x \equiv b' \pmod{n'}$ by c' to get $a'c'x \equiv x \equiv b'c' \pmod{n'}$. This allows us to conclude that x is unique modulo n', but not necessarily unique modulo $n = n'd$. Solutions modulo $n : x, x + n', x + 2n' \ldots, x + (d-1)n'$. Therefore, the congruence will either have there are either 0 or d solutions.

3 Field of fractions

$\mathbb{Z} \subset \mathbb{Q}$. $\mathbb{Z}$ is an integral domain, $\mathbb{Q}$ is a field. There is a little bit more than an integral domain being imbedded in a field, since $\mathbb{Z}$ is also imbedded in $\mathbb{R}$ and $\mathbb{C}$.

Remark 25. $\forall q \in \mathbb{Q}$ can be written as $\frac{n}{m}, n, m \in \mathbb{Z}$

We can call this "the most economical field including $\mathbb{Z}$.

Theorem 26. *Let* R *be an integral domain. Then there exists a field* K*, called is the field of fractions of* R*, such that*

1. R *contained in* K
2. $\forall x \in K$ *can be written as* $x = \frac{r}{s}, r, s \in R$

Understand R in terms of it's field of fractions.

Might be easier to solve Diophantine equations in terms of rationals, then make sense of integral solution.

To prove, we need to

1. Construct K
2. Check that all conditions in the theorem are satisfied

Let S be the set of pairs $(r, s), r, s \in R, s \neq 0$

Define an equivalence relation on S: $(r, s) \sim (r', s')$ if $rs' = r's$

Define K as set of equivalence classes of pairs (r, s)

Check conditions of equivalence relation $\sim$:
$(r, s) \sim (r, s)$ since $rs = rs$
$(r, s) \sim (r's') \iff (r', s') \sim (r, s)$ givens $rs' = r's$ and $r's = rs'$, which are obviously the same
$(r, s) \sim (r', s')$ and $(r', s') \sim (r'', s'') \overset{?}{\implies} (r, s) \sim (r'', s'')$

R integral domain $\implies$ cancelation law

Define L as the set of equivalence classes of pairs (r, s)

Let's define a fraction $\frac{r}{s}$ as the equivalence class of that contains a pair (r, s)

Define binary operations on K

- $\frac{rs' + r's}{ss'}$
- $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$

Need to check that these operations do not depend on which element of the equivalence classes that we select.

Need to check that K satsifies ring axioms
check field axioms

Need to imbedd R

Every element of K is written as a rs^{-1}, with $r, s \in R$