

MATH 412: RINGS AND MODULES

Taught by Jenia Tevelev
Scribed by Ben Burns

UMass Amherst

Spring 2022

CONTENTS

1	Rings and Fields	1
2	Fermat's and Euler's Theorems	2
3	Field of fractions	3
4	Polynomial Rings	4
5	Group Work 2	5
6	Homomorphisms, ideals, quotient rings	5

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). $\text{Mat}_n(\mathbb{R})$ with generic element, addition, and multiplication defined as

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in \text{Mat}_n(\mathbb{R})$$
$$(a_{ij}) + (b_{ij}) = a_{ij} + b_{ij}$$
$$(a_{i1} \dots a_{in}) \cdot \begin{pmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix} = (a_{i1}b_{1j} + \dots + a_{in}b_{nj})$$

Example 6 (Rings of functions). $F = \{f|f : \mathbb{R} \rightarrow \mathbb{R}\}$

$$(f + g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x)g(x)$$

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
 $R \times S = \{(r, s) | r \in R, s \in S\}$.
 $(r, s) + (r', s') = (r + r', s + s')$
 $(r, s)(r', s') = (rr', ss')$

Definition 10. For rings R, S a function $\phi : R \rightarrow S$ 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 $R = \text{Mat}_n(R)$. R 's unity is the identity matrix Id .

$A \in R$ is a unit $\iff AB = BA = \text{Id}$ for some $B \in \text{Mat}_n(R)$

$\iff A$ 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 $n = \text{order}(G)$

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 subtract 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 $d \in \{1, 2, \dots, p - 1\}$ 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 $\{p, 2p, \dots, p^{k-1}p\}$. 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 $1 \leq x \leq r$ coprime to r and $1 \leq y \leq s$ 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 $\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$

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

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

Recall that $\phi(n)$ is the order of \mathbb{Z}_n^* . For $A = \text{order}(x)$, by Corollary to Lagrange, $o \mid \phi(n)$, 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 \mathbb{Z}_p^* has a generator or that \mathbb{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 $d := \gcd(a, n)$, $ax \equiv b \pmod{n} \implies d \mid b$. 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 $\mathbb{Z}_{n'}$. $1 \equiv a'c'$ in $\mathbb{Z}_{n'}$.

Multiply both sides of $a'x \equiv b' \pmod{n'}$ by c' to get $a'c'x \equiv b'c' \pmod{n'}$. This allows us to conclude that x is unique modulo n' , but not necessarily unique modulo $n = n'd$. Solutions modulo n : $x, x + n', x + 2n' \dots, x + (d-1)n'$. 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 $rs = rs$

$(r, s) \sim (r's') \iff (r', s') \sim (r, s)$ gives $rs' = r's$ and $r's = rs'$, which are obviously the same

$(r, s) \sim (r', s')$ and $(r', s') \sim (r'', s'') \xRightarrow{?} (r, s) \sim (r'', s'')$

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 satisfies ring axioms

check field axioms

Need to imbedd R

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

Check distributivity, find what are 0 and 1 in K , check field unit axiom, Embed into K using $i(r) := r/1$

4 POLYNOMIAL RINGS

Definition 27. R is a ring, then $R[X] = \{\text{polynomials in } X \text{ with coefficients in } R\}$
 $= \{a_0 + a_1x + a_2x^2 + \dots | a_i \in R, \text{ finitely many nonzero } a_i\}$

Every $f \in R[X]$ determines a function $R \rightarrow R, r \mapsto f(r) = a_0 + a_1r + a_2r^2 + \dots$

Remark 28. In algebra, two different polynomials can define the same function with coefficients in an arbitrary ring.

$x^p, x \in \mathbb{Z}_p[X], p$ prime. different polynomials, but the functions are the same $\mathbb{Z}_p \rightarrow \mathbb{Z}_p$ because $r^p = r$ because $\forall r \in \mathbb{Z}_p$ by FLT

Suppose $R \subset S$ (subring). $f(x) \in R[X]$. We can also view f as an element of $S[X] \implies$ we can evaluate $f(s), s \in S$. Therefore, we have to be careful to specify what ring we're working with for coefficients.

Definition 29. $f(x) \in R[X]$. $r \in R$ is called a zero of $f(x)$ if $f(r) = 0$. Alternatively called a root.

$x^2 + 1$ has no roots in $\mathbb{R}[X]$, but has two roots in $\mathbb{C}[X], \pm i$

$x^2 - 2 = 0$ has no solution in $\mathbb{Q}[X]$, but has two roots in $\mathbb{R}[X]$

Definition 30 (Rational Zeros Theorem). $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[X]$. If $f(\frac{p}{q}) = 0$, $\gcd(p, q) = 1$, then $p|a_0$ and $q|a_n$.

Lemma 31. $R[X]$ is a ring

$$(a_0 + a_1x + \dots) + (b_0 + b_1x + \dots) = (a_0 + b_0) + (a_1 + b_1)x + \dots$$

$$(R, +) \text{ is an abelian group} \implies (R[X], +) \text{ is an abelian group}$$

$$(a_0 + a_1x + \dots)(b_0 + b_1x + \dots) = (a_0 + b_0) + \left(\sum_{i \geq 0} a_i x^i\right) \left(\sum_{j \geq 0} b_j x^j\right) = \sum_{i,j} a_i b_j x^{i+j}$$

Remark 32. Fix $r \in R$. $R[X] \rightarrow R$ evaluation map, $f(x) \rightarrow f(r)$, is not always a homomorphism unless the ring is commutative

$f(x) \rightarrow f(r), g(x) \rightarrow g(r), f + g \rightarrow f(r) + g(r)$ okay since $+$ abelian, but $fg \rightarrow f(r)g(r)$ may not work if we don't know commutativity holds. $(a_0 + a_1r + \dots)(b_0 + b_1r + \dots) \iff (a_0 + a_1x + \dots)(b_0 + b_1x + \dots)$ with r placed in for x after multiplying polynomials, $a_1rb_1r \neq a_1b_1r^2$ unless R is a commutative ring.

Definition 33. A factorization of $f(x) \in R[X]$ is $f(x) = p_1(x) \cdots p_k(x), p_i \in R[X]$. Suppose R is commutative $\implies p_i(r) = 0$ for some $i \implies f(r) = 0$ (b.c. $f(r) = p_1(r) \cdots p_k(r)$).

If R is an integral domain \implies if $f(r) = 0 \implies p_i(r) = 0$ for some i

Remark 34. Fields are the easiest rings. The next "easiest" ring is $F[X]$, where F is a field

Definition 35 (Long Division of Polynomials). F field, $f, g \in R[X], g \neq 0 \implies$ we can write $f = qg + r$, where $\deg(r) < \deg(g)$ or $r = 0$.

$\mathbb{Z}_5[X]$

5 GROUP WORK 2

Remark 36. If $\phi_p(x)$ has a root in \mathbb{Z}_q , then $\phi_p(x)$ factors as a product of linear factors.

$$x^p - 1 = (x - 1)\phi_p(x) \implies \phi_p(x) \text{ has root } 1 \text{ or has root } \alpha \in \mathbb{Z}_q, \alpha \neq 1.$$

$$\text{If } \phi_p(1) = 1 + 1 + \dots + 1 = p = 0 \pmod{q}, \text{ then } p = q. x^p - 1 \in \mathbb{Z}_p[x] = (x - 1)^p \implies \phi_p(x) = (x - 1)^{p-1}$$

$\phi_p(x)$ has root $\alpha \neq 1 \in \mathbb{Z}_q$. $\alpha^p = 1 \in \mathbb{Z}_q$. \mathbb{Z}_q^* is a cyclic group of order $q - 1$. $\langle \alpha \rangle \subset \mathbb{Z}_q^*$, which has p elements, so $p | q - 1$. Has $\alpha, \alpha^2, \dots, \alpha^{p-1}$, all of which have order p by Corollary to Lagrange. So there are all roots of $x^p - 1 \implies$ they are all roots of $\phi_p(x) \implies \phi_p(x)$ factors as $(x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{p-1})$, which is a product of linear factors.

Start with $f(x) + x^d + \dots \in \mathbb{Z}[x]$. Assume $f(x)$ is irreducible $/\mathbb{Q}$.

Theorem (Chebotarev density Theorem). Every type of the factorization is possible over some \mathbb{Z}_p . This happens infinitely often.

$$\lim_{N \rightarrow \infty} \frac{\# \text{ of all primes } \leq N \text{ with a specific factorization type}}{\# \text{ all primes } \leq N}$$

Irreducible polynomial $x^d + \dots \in \mathbb{Q}[x] \rightarrow$ Galois group $\subset S_d$. Density of primes that give a complete factorization of $f(x)$ into linear factors = $\frac{1}{|\text{Galois group}|}$.

$$G \subset S_5 \mid G \text{ divides } |S_5| = 120. \frac{1}{|G|} \sim \frac{2}{95} \sim \frac{1}{47}.$$

$$x^5 + 2x + 2 \rightarrow \frac{9}{1040} \sim \frac{1}{115} \sim \frac{1}{120} \implies G = S_5$$

6 HOMOMORPHISMS, IDEALS, QUOTIENT RINGS

Definition 37. $\phi : R \rightarrow S$ is a homomorphism of rings iff

- ϕ is a homomorphism of abelian groups with respect to addition: $\phi(a + b) = \phi(a) + \phi(b)$
- $\phi(ab) = \phi(a)\phi(b)$

Definition 38. All the set of all elements $r \in R$ such that $\phi(r) = 0$ is called the **kernel**, which will be an abelian subgroup of the ring R .

Take $r \in R$, $s \in \text{Ker}\phi$. Then $\phi(rs) = \phi(r)\phi(s) = \phi(r)0 = 0 = 0\phi(r) = \phi(s)\phi(r) = \phi(sr)$, so $rs, sr \in \text{Ker}\phi$.

Definition 39. A subset $I \subset R$ is called an **ideal** if

- I is an abelian subgroup with respect to addition
- If $r \in R$ and $s \in I \implies rs, sr \in I$.

Corollary 40. For any homomorphism $\phi : R \rightarrow S$, $\text{Ker}\phi$ is an ideal

Example. The abelian subgroups of \mathbb{Z} are $n\mathbb{Z}$. If you take $r \in \mathbb{Z}$ and $s \in n\mathbb{Z}$, then $s = nk$, and $rs = rnk = n(rk) \in n\mathbb{Z}$.

Corollary 41. All ideals in \mathbb{Z} are of the form $I = n\mathbb{Z}$.

$n\mathbb{Z}$ is the kernel of the homomorphisms $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ where ϕ maps $m \rightarrow m \pmod{n}$

Example. $R_1 \times \{0\} = R_1 \times R_2$ is an ideal as well. $(s, 0) \cdot (r_1, r_2) = (sr_1, 0)$, and $(r_1, r_2) \cdot (s, 0) = (r_1s, 0)$. This is the kernel of $\phi : R_1 \times R_2 \rightarrow R_2$, where ϕ maps $(r_1, r_2) \rightarrow r_2$.

Let R be any ring. Then R always has at least two ideals: R (improper ideal) and $\{0\}$ (trivial ideal).

Remark 42. Every ideal of a field F is either F or $\{0\}$.

Let $I \subset F$ be an ideal. If $I = \{0\}$, we're done. Suppose $I \neq \{0\}$. Then exists $x \in I$. So $x^{-1} \in F \implies x^{-1}x = 1 \in I$. Then take any $y \in F$, $y \cdot 1 = y \in I$. Therefore $F = I$.

Corollary 43. $I \subset R$ is an ideal in a ring with unity. $u \in I$ is a unit $\implies I = R$.

Example. $R = R[x]$, F is a field. $I = \{f \in R : f(1) = 0\}$. This is an ideal, because $f \in F$ and $g \in I$, then $f(1)g(1) = f(1)0 = 0 \in I$. Alternatively, $\phi : F[X] \rightarrow F$ where $\phi(f(x)) \rightarrow f(1)$.

$f(x) \in I \iff f(1) = 0 \iff f(x) = (x-1)g(x) \implies I = \{r(x) : f(x) = (x-1)g(x)\} = (x-1)F[x]$. This looks a *lot* like $n\mathbb{Z}$.

Definition 44. R is a commutative ring. Pick $r \in R$. Then the ideal $I = rR := \{rs : s \in R\}$ is called a **principle ideal**.

I is an abelian group since $rs + rs' = r(s + s') \in I$.

Closure since $rsr' = r'sr = r(r's) \in I$

Definition 45. An integral domain is called a principle ideal domain (PID) if every ideal is principle.

Very good example here being \mathbb{Z} , where all ideals are $I = n\mathbb{Z}$.

Take F to be a field. Two ideals: $\{0\}$ ($0 \cdot F$) and F ($1 \cdot F$), therefore both are principle.

Theorem 46. $R = F[x]$ is a PID for every field F .

Take an ideal $I \subset R$. If $I = \{0\}$, then trivial.

Suppose $I \neq \{0\}$. What is the possible generator of I ? Choose polynomial $f(x) \in I$ of the smallest possible degree.

Claim: Every $g(x) \in I$ is a multiple of $f(x) \implies I = f(x)R[x]$ principle ideal.

$g(x) = f(x)q(x) + r(x)$. Either $r(x) = 0$, and we are done, or $\deg(r) < \deg(f)$. Then $r(x)$ can be written as $g(x) - f(x)q(x) \implies r(x)$ is in the ideal, but this contradicts $r(x)$ having smaller degree than $f(x)$, which is a contradiction. Therefore, $\deg(r) = 0 \implies g(x) = f(x)q(x)$.

Remark 47. ϕ is one to one $\iff \text{Ker}\phi = \{0\}$

Because this is true for homomorphisms of abelian groups.