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 $R = Mat_n(R)$. R's unity is the identity matrix Id.
$A \in R$ is a unit $\iff AB = BA = Id$ for some $B \in Mat_n(R)$
$\iff$ 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 $n = order(G)$

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 $d \in \{1, 2, \dots p-1\}$ 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 $1 \leqslant x \leqslant r$ 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 $\mathbb{Z}_{\prime}$

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 $n : x, x + n', x + 2n' \dots, x + (d-1)n'$. 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 $\dfrac{n}{m}, n, m \in \mathbb{Z}$

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* $x = \dfrac{r}{s}, r, s \in R$

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 $\dfrac{r}{s}$ as the equivalence class of that contains a pair (r, s)

Define binary operations on K

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

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 $r, s \in R$

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

4 Polynomial Rings

Definition 27. R is a ring, then R[X] = {polynomials in X with coefficients in R}
= $\{a_0 + a_1 x + a_2 x^2 + \ldots | a_i \in R$, finitely many nonzero $a_i\}$

Every $f \in R[X]$ determines a function $R \to R, r \to f(r) = a_0 + a_1 r + a_2 r^2 + \ldots$

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 $\mathbb{Z}_p \to \mathbb{Z}_p$ beacuse $r^p = r$ 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)**.** $f(x)=a_0+a_1x+\ldots+a_nx^n \in \mathbb{Z}[X]$. 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*

$(a_0+a_1x+\ldots)+(b_+b_1x+\ldots)=(a_0+b_0)+(a_1+b_1)x+\ldots$
$(R,+)$ is an abelian group $\implies$ $(R[X],+)$ is an abelian group
$(a_0+a_1x+\ldots)(b_+b_1x+\ldots)=(a_0+b_0)=(\sum_{i\geqslant 0} a_ix^i)(\sum_{j\geqslant 0} b_jx^j)=\sum_{i,j}=a_ib_jx^{ij}$

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

$f(x)\to f(r), g(x)\to g(r), f+g\to f(r)+g(r)$ okay since $+$ abelian, but $fg\to f(r)g(r)$ may not work if we don't know commutativity holds. $(a_0+a_1r+\ldots)(b_0+b_1x+\ldots) \iff (a_0+a_1x+\ldots)(b_0+b_1r+\ldots)$ 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 fr) $=p_1(r)\cdots p_k(r)$.

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.

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

If $\phi_p(1)=1+1+\ldots+1=p=0 \pmod q$, 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 $q-1$. $<\alpha>\subset\mathbb{Z}_q^*$, which has p elements, so $p|q-1$. Has $\alpha,\alpha^2,\ldots,\alpha^{p-1}$, 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 $(x-\alpha)(x-\alpha^2)\cdots(a-\alpha^{p-1})$, which is a product of linear factors.

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

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

$$\lim_{N\to\infty}\frac{\#\textit{ of all primes } \leqslant N \textit{ with a specific factorization type}}{\#\textit{ all primes } \leqslant N}$$

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

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

$x^5+2z+2\to\dfrac{9}{1040}\sim\dfrac{1}{115}\sim\dfrac{1}{120} \implies G=S_5$

6 Homomorphisms, Ideals, and Quotient Rings

6.1 Homomorphisms

Definition 37. $\phi : R \to S$ 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 $rs, sr \in \text{Ker}\phi$.

6.2 Ideals

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 $s \in R \implies rs, sr \in I$.

Corollary 40. *For any homomorphism* $\phi : R \to S$, *Ker*ϕ *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 $\phi : \mathbb{Z} \to \mathbb{Z}_n$ where ϕ maps $m \to m \pmod n$

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 $(r_1,r_2)\cdot(s,0) = (r_1 s,0)$. This is the kernel of $\phi : R_1 \times R_2 \to R_2$, where ϕ maps $(r_1,r_2) \to r_2$.

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, $\phi : F[X] \to F$ where $\phi(f(x)) \to f(1)$.

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

Definition 44. R is a 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 $rsr' = r'rs = r(r's) \in I$

Definition 45. An integral domain is called a **principle ideal domain** a(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.

Definition 48. For ring R and ideal $I \subset R$ such that $I \neq R$, I is called **maximal** if every ideal J such that $I \subset J \subset R$ is either I or R.

Example. $\{0\} \subset F$ field, $p\mathbb{Z} \subset \mathbb{Z}$ where p prime.
$F[x]$, for F field, is a principle ideal domain. Take $f(x)F[x] \subset F[x]$, where $f(x)$ is an irreducible polynomial $\implies f(x)F[x]$ is a maximal ideal

Example 49. Compute $\mathbb{Z}_2[x]/(x^2 + x + 1)F[x]$.

What are the cosets? Take $g(x) \in \mathbb{Z}_2[x]$ and take its coset $g(x) + x^2 + x + 1$.

Claim: there are only four cosets. The ideal itself I, $1 + I$, $x + I$, $(1 + x) + I$

Take any coset $g(x) + I$. Perform long division $g(x) = (x^2 + x + 1)q(x) + r(x)$, where $deg(r) < 2$. All possible $r(x)$ are 0, 1, x, $x + 1$.

7 Unique Factorization Domains

Define R to be an integral domain.

Definition 50. For $p \in R$ irreducible, if $p = ab \implies a$ or b is a unit

Definition 51. If $(p) \subset R$ is a prime ideal, then $p \in R$ prime.

Recall Euclid's Lemma: $p|ab \implies p|a$ or $p|b$ $\forall a, b \in R$

Remark 52. If p is prime then p is irreducible

Definition 53. An integral domain R is called a unique factorization domain (UFD) if
1) Every element can be written as $r = up_1p_2 \cdots p_r$ where u is a unit and p_i are irreducible elements
2) Suppose $up_1 \cdots p_r = vq_1 \cdots q_s$, with u, v unit, everything else irreducible, then $r = s$ and after reordering $q_1 \dots q_s$, $p_i = q_i \cdot u)i$ for some unit u_i

Remark 54. If R is a UFD, then every irreducible element is prime

$r \in R$ irreducible. Suppose $r|ab$, then $ab = pc, c \in R$. Apply factorization to a, b, c: $(up_1 \dots p_r)(vq_1 \dots q_s) = p(wl_1 \dots l_k)$, u, v, w are units

Uniqueness of factorization $\implies p_i = \alpha p$ or $q_i = \alpha p$ for for some i, unit α.

In the first case, then $a = up_1 \dots p_{i-1}(\alpha p)p_{i+1} \cdots p_r \implies p|a$

Remark 55. Suppose R is an an integral domain where factorization exists. $\implies$ one can conclude that, if every irreducible unit is prime, then R is a UFD

Suppose $up_1 \cdots p_r = vq_1 \cdots q_s$, with u, v unit. Then $p_1|vq_1 \dots q_s$. $p_1 \nmid u \implies p_1|q_i$ for some i. (Because p_1 is irreducible, and here all irreducibles are prime). By rearranging, $p_1|q_1$, so $p_1\beta = q_1$. q_1 irreducible implies β must be a unit. Cancel p_1 using integral domain cancelation law: $up_2 \dots p_r = (v\beta)q_2 \dots q_s$. By induction, we are done.

Example. $K[X]$ is a UFD if K is a field.

(1) $f(x) \in K[x]$ is irreducible. We already checked that $f(x)K[x]$ is maximal. But every maximal ideal is prime $\implies f(x)$ is a prime element.

(2) Show existence of factorization: take polynomial $f(x) \in K[x]$. Argue by induction on $deg(f(x))$. If $f(x)$ is unit $\iff deg(f(x)) = 0 \implies$ factorization exists. If $f(x)$ is irreducible $\implies$ factorization exists. Else, $f(x) = g(x)h(x)$ for $0 < deg(g(x)), deg(h(x)) < deg(f(x))$. Both admit factorizations by induction, so combine then to get factorization.

Suppose $r = r_1$ does not allow factorization $\implies r_1$ is not a unit, not irreducible $\implies r = ab$, where a, b not units. One of them, say $a = r_2$ does not allow factorization. $r_1 = r_2b_2$, b_2 is not a unit. Can continue inducting, and get a sequence $r_i = r_{i+1}b_{i+1}$ where all $r_1, r_2, \ldots$ do not allow factorization and $b_1, b_2, \ldots$ are not units.

Take (r_1) and (r_2). $(r_1) \subset (r_2) \subset (r_3) \subset \ldots$. Can it be that $(r_1) = (r_{i+1})$? No. Then $r_i = r_{i+1}b_{i+1}$ and $r_{i+1} = r_ic_i \implies r_i = r_ib_{i+1}c_i \implies 1 = b_{i+1}c_i \implies b_{i+1}$ is a unit, contradiction.

$(r_1) \subsetneq (r_2) \subsetneq (r_3) \subsetneq \ldots$

Definition 56. A commutative ring R is called Noetherian if there are no infinite ascending chains of ideals $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$

Corollary 57. *If R is Noetherian integral domain where irreducible elements are prime, then it's a UFD*

8 Field Extensions

$K \subset F$, towers of fields: $K_1 \subset K_2 \subset K_3$

K field, $f(x) \in K[x]$ irreducible polynomial. Take $I = f(x)$ maximal ideal. $F = K[X]/I$ is a field.

Theorem 58. $K \to K[x] \to K[x]/I = F \implies K \to F$ *by composition.* $f(x)$ *has a root* $\alpha \in F$

Corollary 59. *If you take any polynomial in* $f(x) \in K[x]$, *factors into linear factors in some field extension of* $K \subset F$

Proof: $K \overset{\phi}{\to} F$. Kerϕ is an ideal of K, K is a field, either Ker$\phi = \{0\}$ (and ϕ is injective) or Ker$\phi = K$. But that can't happen because $1 \in K \to 1 \in K[x] \to 1 + I$, a unity in F, which is certainly not zero, so $\phi(1) \neq 0$, and I must be $\{0\} \implies K \to F$

Claim: $x + I = \alpha \in F$ is going to be a root of $f(x)$ $f(x + I) = f(x) + I = I = 0 \in F$. If confused, try plugging in $x + I$ and doing it out.

$x^2 + 1 \in \mathbb{R}[x]$, $I = (x^2 + 1)$. $\mathbb{R}[x]I = \{p(x) + I\} = \{p(x) = I : deg(p < 2)\}$. Indeed $p(x) = (x^2 + 1)q(x) + r(x) \implies p(x) + I = r(x) + I$ because $p(x) - r(x) = q(x)(x^2 + 1) \in I$. Morever, every coset can be written uniquely as $\{a + bx + I\}$ where $a, b \in \mathbb{R}$.

Definition 60. Let $K \subset K$ be a field extension. Choose some $\alpha \in F$. α is **algebraic** over K if there exists $f(x) \in K[x]$ such that $f(\alpha) = 0$.

Definition 61. Any element that is not algebraic is **transcendental** over K

Example. Consider $\mathbb{Q} \subset \mathbb{C}$. Algebraic $\alpha \in \mathbb{C}$ over $\mathbb{Q}$ are called algebraic (transcendental) numbers.

Theorem 62. e, π *are transcendental over* $\mathbb{Q}$

Very hard to prove. Much easier to prove numbers are algebraic

Remark 63. If you have a trivial field extension $F \subset F$, then all elements will be algebraic

In a real analysis context, algebraic and transcendental are with rational coefficients, so π and e are transcendental. For the extension $\mathbb{R} \subset \mathbb{R}$ and $\mathbb{R} \subset \mathbb{C}$ both are now algebraic, since $x - \pi = 0$ has π as a solution, and $x - e = 0$ has e as a solution.

Lemma 64. *Suppose $K \subset F$ field extension. Take $\alpha \in F$ algebraic $\implies$ there exists a unique minimal (aka irreducible) polynomial irr(α, K) which is*
1) irreducible and nonzero
2) has α as a root
3) and monic

$irr(\alpha, K)$ is the minimal polynomial of α over K.

The main tool to prove this is the evalutation homomorphism. $\phi : K[x] \to F$ which sends $f(x) \to f(\alpha)$.

$I = \text{Ker}(\phi) \subset K[x]$ ideal. By definition, it is $= \{f \in K[x] : f(\alpha) = 0\}$. $I \neq 0 \iff \alpha$ is algebraic $/K$, and $I = 0 \iff \alpha$ is transcendental $/K$.

Case 1: $I \neq 0 \iff \alpha$ is algebraic. The ideal I is principle: $I = (f)$. Rescale f by a constant to make it monic. Why is it irreducible? If $f(x) = a(x)b(x)$ with $deg(a), deg(b) < deg(f)$. $f(\alpha) = a(\alpha)b(\alpha) = 0$, but then at least one of them has to be in the ideal, but they can't be since they have degree less than f (because we selected f to be the generating polynomial). Therefore $\mathrm{irr}(\alpha, K)$ exists.

Why is it unique? Suppose $g(x)$ also satisfies the three conditions. Therefore, $g(\alpha) = 0$, so $g(x)$ is in the ideal $I = (f)$. But then $g(x) = f(x)q(x)$. But $g(x)$ is irreducible, so $q(x)$ has to be a constant, else $g(x)$ has a nontrivial factorization, and must be 1 else one of $f(x)$ or $g(x)$ isn't monic.

Example. $\mathrm{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, $\mathrm{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$.

Definition 65. Suppose $K \subset F$ fields, $\alpha \in F$. A **simple field extension** $K(\alpha)$ is the smallest subfield of F that contains K and α. Generalization: $K(\alpha, \beta)$ contains K, α, and β.

$\phi : K[x] \to F$, $I = \mathrm{Ker}\phi$. $I \neq 0 \iff \alpha$ algebraic/K
$\implies I = (f)$, where $f = \mathrm{irr}(\alpha, K)$

Apply the first isomorphism theorem:

$$\begin{tikzcd}
K[x] \arrow[r, "\phi"] \arrow[d] & F \\
K[x]/I \arrow[r, "\simeq"] & \mathrm{Im}\phi \arrow[u, "\cup"']
\end{tikzcd}$$

$\implies \mathrm{Im}\phi$ is a subfield, isomorphic to $K[x]/I$, contains J, $\alpha = \phi(x)$.

Claim: $\mathrm{Im}(\phi) = K(\alpha)$. Why is it the smallest? Suppose N is a subfield of F that contains K and α. Is $\mathrm{Im}(\phi) \in N$? Yes, $\phi(a_0 + \ldots + a_n x^n) = a_0 + \ldots a_n a^n \in N$

Case 2: $\phi : K[x] \to F$ which sends $p(x) \to p(\alpha)$. $I = \mathrm{Ker}\phi = 0 \implies \phi$ is injective.

$K[x] \xrightarrow{\phi} F \implies K(x) = \{\frac{p(x)}{q(x)} : p, q \in K[x]\}$ is also contained in $F \implies K(\alpha) \cong K[x]$

9 Linear algebra over a field K

Vector space of column vectors $\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$, $a_i \in K$

Two operations: $\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{bmatrix}$
and $k \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} ka_1 \\ \vdots \\ ka_n \end{bmatrix}$

These operations satisfy axioms of vector space $/K$.

Set V with 2 operations:
$V \times V \to V$, sends $u, v \to u + v$, and $K \times V \to V$ sending $k, v \to ku$ subject to axioms:

- $(V, +)$ is an abelian group, in particular we have a zero vector $0 \in V$
- distributivity $k(u + v) = ku + kv$ and $(k + k')u = ku + k'u$
- "action" or "associativity" $l(ku) = (lk)u$, and $1 \cdot v = v$

Example. Suppose we have a field extension $K \subset F$. Then we have $f_1 + f_2$, $f_1, f_2 \in F$, and can compute kf, for $k \in K$ and $f \in F$. Therefore, as a consequence of ring axioms, F satisfies the axioms of a vector space over a field K.

Example. $R \subset C$

View $\mathbb{C}$ as a vector space over $\mathbb{R}$, with basis vectors 1 and i.

Remark 66. We can imbed field K into a ring R and this still holds since we used ring axioms only.

Definition 67. Suppose we have V vector space/K, with $v_1, \ldots, v_k \in V$. We say $v_1, \ldots, v_k$ **span** V if $\forall v \in V$ can be written $v = \sum a_i v_i$ for $a_i \in K$.

Definition 68. $v_1, \ldots v_k$ are **linearly independent** if $\sum a_1 v_1 = 0 \implies \forall a_i = 0$.

Definition 69. $\{v_1, \ldots, v_k\}$ is a **basis** if they span and are linearly independent.

Lemma 70. *$v_1, \ldots, v_n$ span V and $u_1, \ldots, u_k$ are linearly independent, then $k \leqslant n$.*

Corollary 71. *If V has a finite basis with n vectors, then every other basis also has n vectors. This n is called the* ***dimension*** *of V over K (otherwise $\mathrm{dim} V = \infty$)*

Example. dim $\mathbb{C}$ over $\mathbb{R}$ is 2 with basis 1 and i

$\alpha \in \mathbb{C}$, $\alpha = a \cdot 1 + b \cdot i, a, b \in \mathbb{R} \implies 1, i$ span $\mathbb{C}$

$a, b \in \mathbb{R}, a + bi = 0 \implies a = b = 0 \implies 1$ and i are linearly independent.

Definition 72. $K \subset F$ a field extension $\implies F$ vector space/K. Then the dimension of F over K is called the **degree** of the field extension, notated $[F : K]$