

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, and Quotient Rings | 6 |
| 6.1 | Homomorphisms | 6 |
| 6.2 | Ideals | 6 |
| 7 | Unique Factorization Domains | 7 |
| 8 | Field Extensions | 8 |
| 9 | Linear algebra over a field K | 9 |
| 10 | Algebraic Extensions | 11 |
| 11 | Geometric Constructions | 13 |
| 12 | Finite Fields | 14 |
| 13 | Group Work 6 | 15 |

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 multiplication defined as

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in Mat_n(\mathbb{R})$$

$$(a_{ij}) + (b_{ij}) = a_{ij} + b_{ij}$$

$$(a_{i1} \quad \dots \quad a_{in}) \cdot \begin{pmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix} = (a_{i1}b_{1j} + \dots + a_{in}b_{nj})$$

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 $\iff AB = BA = Id$ 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 preceding 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 $n = p_1^{k_1} \dots p_r^{k_r}$. Then $\phi(n) = \phi(p_1^{k_1}) \dots \phi(p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1-1}) \dots (p_r^{k_r} - p_r^{k_r-1})$

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, $o|\phi(n)$, 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}_p^* 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 $\mathbb{Z}_{n'}$. $1 \equiv a'c' \pmod{n'}$

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 $\frac{n}{m}$, $n, m \in \mathbb{Z}$

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

$$\begin{aligned} &\bullet \frac{rs' + r's}{ss'} \\ &\bullet \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'} \end{aligned}$$

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

$$\begin{aligned} (a_0 + a_1x + \dots) + (b_0 + b_1x + \dots) &= (a_0 + b_0) + (a_1 + b_1)x + \dots \\ (R, +) \text{ is an abelian group} &\implies (R[X], +) \text{ is an abelian group} \\ (a_0 + a_1x + \dots)(b_0 + b_1x + \dots) &= (a_0 + b_0) = \left(\sum_{i \geq 0} a_i x^i\right) \left(\sum_{j \geq 0} b_j x^j\right) = \sum_{i,j} a_i b_j x^{ij} \end{aligned}$$

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 $fr = p_1(r) \cdots p_k(r)$).

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 $\phi_p(1) = 1 + 1 + \dots + 1 = p = 0 \pmod{q}$, 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 $q - 1$. $\langle \alpha \rangle \subset \mathbb{Z}_q^*$, 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 = $\frac{1}{|\text{Galois group}|}$.

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

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

6 HOMOMORPHISMS, IDEALS, AND QUOTIENT RINGS

6.1 Homomorphisms

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 $rs, sr \in \text{Ker}\phi$.

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

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 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 $rsr' = r's = r(r's) \in I$

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.

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 $q_1 \cdots q_s$, $p_i = q_i \cdot u_i$ 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 : $(up_1 \cdots p_r)(vq_1 \cdots q_s) = p(wl_1 \cdots l_k)$, u, v, w are units

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

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

Remark 55. Suppose R is 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 $p_1|vq_1 \cdots q_s$. $p_1 \nmid v \implies p_1|q_i$ 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: $up_2 \cdots p_r = (v\beta)q_2 \cdots q_s$. 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 them 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. $r_1 = r_2 b_2$, 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, \dots do not allow factorization and b_1, b_2, \dots are not units.

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

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

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

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

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 $p(x) - r(x) = q(x)(x^2 + 1) \in I$. Moreover, every coset can be written uniquely as $\{a + bx + I\}$ where $a, b \in \mathbb{R}$.

Definition 60. Let $K \subset F$ 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 $\text{irr}(\alpha, K)$ which is

- 1) irreducible and nonzero
- 2) has α as a root
- 3) and monic

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

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

$I = \text{Ker}(\phi) \subset K[x]$ 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 $\text{irr}(\alpha, K)$ 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. $\text{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, $\text{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$.

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 .

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

Apply the first isomorphism theorem:

$$\begin{array}{ccc} K[x] & \xrightarrow{\phi} & F \\ \downarrow & & \uparrow \\ K[x]/I & \xrightarrow{\cong} & \text{Im}\phi \end{array}$$

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

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

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

$K[x] \xrightarrow{\phi} F \implies K(x) = \left\{ \frac{p(x)}{q(x)} : p, q \in K[x] \right\}$ 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:

$V \times V \rightarrow V$, sends $u, v \rightarrow u + v$, and $K \times V \rightarrow V$ sending $k, v \rightarrow kv$ 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. $\mathbb{R} \subset \mathbb{C}$

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 $v_1, \dots, v_k \in V$. We say v_1, \dots, 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, \dots, v_k are **linearly independent** if $\sum a_i v_i = 0 \implies \forall a_i = 0$.

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

Lemma 70. v_1, \dots, v_n span V and u_1, \dots, u_k are linearly independent, then $k \leq n$.

$u_i = \sum_{j=1}^n a_{ij} v_j$. Argue by contradiction. Suppose $k > n$. Leters try to find a nontrivial linear combination (all terms nonzero) $x_1 u_1 + \dots x_k u_k = 0$ $x_i \in K$.

$$\implies \sum_{i=1}^k x_i u_i = 0$$

$$\implies \sum_{i=1}^k x_i \sum_{j=1}^n a_{ij} v_j = 0$$

$$\implies \sum_{i=1}^k \sum_{j=1}^n x_i a_{ij} v_j = 0$$

Certainly true if $\sum_{i=1}^k x_i a_{ij} = 0 \forall j = 1, \dots, n$. We have a system of n homogeneous linear equations in k variables x_1, \dots, x_k , and $k > n$. Therefore, it has a nontrivial solution.

Run row reduction, we have > 0 independent variables, which can take arbitrary values.

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 $\dim V = \infty$)

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

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

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

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 $[F : K]$

Lemma 73. $f(x) \in K[x]$ irreducible of degree n . $I = (f) \subset K[x]$, $F = K[x]/I$. Then $[F : K] = n$, easy to write a basis as well.

$\alpha = X + I \in F$. Claim: $1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{n-1}$ is a basis of F over K , with dimension n .

$F = K[x]/I \implies$ elements of F are cosets $p(x) + I$, $p(x) \in K[x]$. Recall $p(x) = f(x)q(x) + r(x)$, degree of $r < \deg f$. $I = (f(x))$, $f(x)q(x) \in I$, $p(x) + I = r(x) + I$.

If $r(x)$ and $r'(x)$ give the same coset, then $r(x)$ must be equal to $r'(x)$, since $r(x) - r'(x) \in I \implies r(x) - r'(x) = f(x)s(x) \implies \deg(r - r') < \deg(f) \implies r = r' \implies$ we can write every element of F as $a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + I$, $a_i \in K$ uniquely. $a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1} = a_0(1 + I) + a_1(x + I) + \dots + a_{n-1}(x + I)^{n-1} =$ above.

Therefore, $\{1, \alpha, \dots, \alpha^{n-1}\}$ is a basis, since every element of F is a unique linear combination of $1, \dots, \alpha^{n-1}$ with coefficients in K .

Corollary 74. $K \subset F$ field extension, $\alpha \in F$ algebraic over K with minimal polynomial of degree $n \implies [K(\alpha), K] = n$, with basis $\{1, \alpha, \dots, \alpha^{n-1}\}$.

$f(x) = \text{irr}(\alpha, K)$. Last time: $K(\alpha) \cong F/(f)$ with α matched with $x + I$.

Example. $K = \mathbb{Q}, \alpha \in \mathbb{C}$, study $K(\alpha)$?

$$\mathbb{Q}(\sqrt{2}), \text{irr}(\sqrt{2}) = x^2 - 2 \implies [\mathbb{Q}(\sqrt{2}), \mathbb{Q}] = 2, \text{ with basis } 1, \sqrt{2}.$$

Therefore, $\forall x \in \mathbb{Q}(\sqrt{2})$ can be written uniquely as $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$.

Example. $\mathbb{Q}(\sqrt{1+\sqrt{3}})$

$\alpha^2 = 1 + \sqrt{3} \implies \alpha^2 - 1 = \sqrt{3} \implies (\alpha^2 - 1)^2 = 3 \implies \alpha^4 - 2\alpha^2 - 2 = 0$. Is irreducible by Eisenstein with $p = 2$. Therefore, $[\mathbb{Q}(\alpha), \mathbb{Q}] = 4$, basis is $1, \alpha, \alpha^2, \alpha^3$

How to write $\frac{1}{1 + \alpha + \alpha^2}$ as linear combination?

$x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3$, solve for x_0, \dots, x_4 . $1 = (1 + \alpha + \alpha^2)(x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3)$. $\alpha^4 = 2\alpha^2 + 2$. Multiply out, and substitute in for α^4 at each step to only use powers of $\alpha < 4$. Gives a system of 4 equations in four variables.

10 ALGEBRAIC EXTENSIONS

Definition 75. A field extension $K \subset F$ is called **algebraic** if every element $\alpha \in F$ is algebraic/ K .

Theorem 76. Every finite extension is algebraic

$[F : K] = n, \alpha \in F$. Basis $e_1, e_2, \dots, e_n \in F$. Take $1, \alpha, \dots, \alpha^n$. Are linearly dependent $\implies x_0 + x_1\alpha + \dots + x_n\alpha^n = 0$ for some $x_i \in K$, not all 0, so $P(\alpha) = 0$.

Example. $\mathbb{Q}(2^{a/3})$

$[\mathbb{Q}(2^{a/3}) : \mathbb{Q}] = 3$ since $x^3 - 2 = 0$, irr by Eisenstein
 $\implies \forall p \in \mathbb{Q}(2^{1/3})$ is algebraic over \mathbb{Q}

Take $\beta = 1 + 2^{1/3} + 2(2/3)$. Basis of $\mathbb{Q}(2^{1/3})$ is $\{1, 2^{1/3}, 2^{2/3}\}$. Compute $1, \beta, \beta^2, \beta^3$ as linear combinations of $1, 2^{1/3}, 2^{2/3} \implies$ set-up a linear combination with unknown coefficients $x_0 + x_1\beta + x_2\beta^2 + x_3\beta^3$ in terms of the basis. Solve a SLE with 4 variables and 3 equations.

Remark 77. Suppose α is algebraic over F . Then $F(\alpha) \cong F[x]/(f)$ where $f(x)$ is the irreducible polynomial. We have a basis of $F(\alpha)$ over F given by $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$, where n is the degree of $f(x) = [F(\alpha) : F]$

Theorem 78 (Transitivity of degree). $F \subset K \subset L$ fields. Suppose L is a finite extension of F . Then $[L : F] = [L : K][K : F]$

Proof: Choose a basis $\alpha_1, \dots, \alpha_n$ of K as a vector space over F . Choose β_1, \dots, β_m of L as a vector space over K . Claim $\alpha_i\beta_j$ for $i = 1, \dots, n$ and $j = 1, \dots, m$ is a basis of L over F .

Have to check that

- (1) every element $\gamma \in L$ can be written as a linear combination of $\alpha_i\beta_j$ with coefficients in F
- (2) These vectors are linearly independent over F .

Well, the β terms being a basis of L over K means that $\gamma = \sum_{j=1}^m k_j\beta_j$. But the α terms form a basis of K over F ,

so each $k_j = \sum_{i=1}^n f_{ij}\alpha_i$. Therefore, you can substitute in the summations to get $\gamma = \sum_{j=1}^m \sum_{i=1}^n f_{ij}a_ib_j$. so we have part (1).

(2) Claim: $\alpha_i\beta_j$ are linearly independent over F . Write $\sum_{i,j} f_{ij}\alpha_i\beta_j = 0$. To show linear, independence, we must show that all f_{ij} are 0.

Well, this implies that $\sum_{j=1}^m (\sum_{i=1}^n f_{ij}\alpha_i)\beta_j = 0$, but the β terms form a basis, so are linearly independent with each summation term being in K , so each summation w.r.t j equals 0. Well, by the same logic, since α are all linearly independent, all f_{ij} must be zero, and we are done.

Corollary 79. If $[L : F]$ is prime, then either $[L : K] = 1 \implies L = K$ or $[K : F] = 1 \implies K = F$

Example. $[\mathbb{Q}(2^{a/3}) : \mathbb{Q}] = 3$

$\beta = 1 + 2^{1/3} + 2^{2/3}$. Then, take $\mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$. Then either $\mathbb{Q} = \mathbb{Q}(\beta)$ or $\mathbb{Q}(\beta) = \mathbb{Q}(2^{1/3})$. The latter must be true, since β is not rational $\implies \deg(\text{irr}(\beta, \mathbb{Q})) = [\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$

Example. $\mathbb{Q}[\sqrt{2}]$

Has degree 2, since irreducible polynomial is $x^2 - 2$. Take $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ over $\mathbb{Q}[\sqrt{2}]$ has degree two because the irreducible polynomial is $x^2 - 3$

Is this irreducible? Well if not, then there is a root, namely $\sqrt{3}$ so then $\sqrt{3} \in \mathbb{Q}[\sqrt{2}]$, so $\sqrt{3} = a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$. Square both sides, get $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, which can't be true unless a is zero or b is zero.

If b is zero, then $\sqrt{3} = a$, but we know it's irrational. If a is zero, then we have $\sqrt{3} = b\sqrt{2}$, or $2b^2 - 3 = 0$, which is irreducible by Eisenstein, so b is irrational if the two sides are indeed equal.

Therefore, $[\mathbb{Q}(\sqrt{2}, \sqrt{3})]$ has degree 4, with basis $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. This is a simple field extension, since we've already checked that $x^4 - 10x^2 + 1$ is an irreducible polynomial with degree 4 with $\sqrt{2} + \sqrt{3}$ as a root.

Therefore, we have $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, where the first extension has degree 4, and the whole extension has degree 4, so the right two must be equal, and the last field must have degree 4 over \mathbb{Q}

Example. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$

$F \subset K$ field extension. Consider $L = \{\alpha \in L : \alpha \text{ is algebraic over } F\}$ If $F \subset K$ is algebraic $\implies L = K$.

Lemma 80. L is a subfield of K , called an **algebraic closure** of F in K

Example. $\mathbb{Q} \subset \mathbb{C}$. Algebraic closure of $\mathbb{Q} \in \mathbb{C}$ is denoted $\overline{\mathbb{Q}}$, field of algebraic numbers

Proof of lemma: $\forall, \alpha, \beta \in L$, check that $\alpha\beta$, $\alpha - \beta$, and α/β is in L . Meaning, these three should also be algebraic over K .

Consider extension $K \subset K(\alpha)$, which is finite. Then extension $K(\alpha) \subset K(\alpha, \beta)$, which is also finite since β is algebraic over K . Therefore $K \subset K(\alpha, \beta)$ is also finite with degree of product of the subdegrees. Because this extension is finite, it must be algebraic $\implies \alpha \pm \beta, \alpha\beta, \alpha/\beta$ are algebraic over K

Remark 81. How can we find a

Example. $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$ is an algebraic closure, and is therefore automatically a field without having to prove it specifically

Definition 82. An algebraic closure \overline{K} of a field K is a field extension of K such that

1. $\forall \alpha \in \overline{K}$ is algebraic over K

2. \overline{K} is algebraically closed, which means that every polynomial in $\overline{K}[x]$ has a root in \overline{K}

(2) \iff every polynomial in $\overline{K}[x]$ factors into linear factors in $\overline{K}[x]$

Example. \mathbb{C} is algebraically closed $\implies \mathbb{C}$ is an algebraic closure of \mathbb{R}

(1) \mathbb{C} is algebraically closed

(2) $a + bi \in \mathbb{C}$ is algebraic over \mathbb{R} ? $(x - a - bi)(x - a + bi) = x^2 - 2ax + (a^2 + b^2)$

Example. $\overline{\mathbb{Q}}$ is algebraically closed

Example. $c = \sum_{n \geq 1} \frac{1}{10^n n!}$

Last time: c is a Liouville number, which means that $c \notin \mathbb{Q}$, and $\forall n \geq 1, \exists \frac{p}{q} \in \mathbb{Q}$ such that $\left|c - \frac{p}{q}\right| \leq \frac{1}{q^n}$

Lemma 83. Liouville numbers are transcendental ($\notin \mathbb{Q}$)

Argue by contradiction > Suppose that a Liouville number α is algebraic/ \mathbb{Q} . Well, then there exists an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. Rescale the polynomial by the lcm of the denominators such that $f(x) \in \mathbb{Z}[x]$

$f(\alpha) = 0$, but $f(\frac{p}{q}) \neq 0$ because $f(x)$ is irreducible/ \mathbb{Q}

$f(x) = a_0 x^m + a_1 x^{m-1} + \dots + a_m$ with $a_i \in \mathbb{Z}$.

$\left|f\left(\frac{p}{q}\right)\right| = \left|a_0 \frac{p^m}{q^m} + \dots + a_m\right| \geq \frac{1}{q^m}$ because $= \left|\frac{a_0 p^m + a_1 p^{m-1} q + \dots + a_m q^m}{q^m}\right|$

Choose $\frac{p}{q}$ such that $\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^n}$. Then $f(\alpha) - f(\frac{p}{q}) = f'(x)(\alpha - \frac{p}{q})$ for x between α and $\frac{p}{q}$

$$\left| f(\alpha) - f(\frac{p}{q}) \right| = |f'(x)| \left| \alpha - \frac{p}{q} \right|$$

$|x - \alpha| \leq 1$ because $\left| \frac{p}{q} - \alpha \right| < \frac{1}{q^n} \leq 1$. Let M be the $\sup_{|x-\alpha| \leq 1} |f'(x)|$, so

$$\frac{1}{q^m} \leq \left| f(\frac{p}{q}) \right| = \left| f(\alpha) - f(\frac{p}{q}) \right| \leq M \left| \alpha - \frac{p}{q} \right| \leq M \frac{1}{q^n}$$

$\implies \frac{1}{q^m} \leq \frac{M}{q^n} \implies q^n \leq M q_a^m \implies 2^{n-m} \leq q^{n-m} \leq M$. This obviously can't be true for all n

11 GEOMETRIC CONSTRUCTIONS

What can be constructed with a straightedge and a compass

Classical problems

1. Doubling the cube (basically, can we construct cube root of 3)
2. Trisect angle
3. Squaring the circle (circle with area A to square with area A)

Algebraic interpretation: Let's define field $K \subset \mathbb{R}$ to be a field of all numbers x such that the segment of length x can be constructed with straightedge and compass starting with a segment of length 1.

You can take α and β and get $\alpha + \beta$

Start with $1 \rightarrow \mathbb{Q}$. Easy.

Take $a + 1$, then half circle, then get altitude, which has length \sqrt{a} . Then we can adjoin \mathbb{Q} with any square root.

Let's call $\alpha \in \mathbb{R}$ constructible if it can be constructed using straightedge and compass.

Theorem 84. $\alpha \in \mathbb{R}$ is constructible \iff there exists $\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_r$ such that $K_r = K_{r-1}(\sqrt{\beta_r})$, where $\beta_r \in K_{r-1}$

We already just proved one direction.

For the other way, we can formalize "straightedge and compass" as we can create a series of points $(x_n, y_n) \in \mathbb{R}^2$ with starting points $(x_1, y_1) = (0, 0)$ and $(x_2, y_2) = (1, 0)$.

What can (x_n, y_n) be? Either (x_n, y_n) is an intersection point of a line passing through $(x_i, y_i), (x_j, y_j)$ and a line through (x_k, y_k) and (x_l, y_l) for $i, j, k, l < n$, or we can use circles with center (x_i, y_i) and passint through $(x_j, y_j), i, j < n$.

Claim: we can compute (x_n, y_n) using x_i, y_i for $i < n$ using $+, -, \cdot, /$ and $\sqrt{}$

$y - y_i = \frac{y_j - y_i}{x_j - x_i}(x - x_i)$ or $x = x_i$ if $x_i = x_j$, so a line $y = kx + b$ or vertical lines.

To intersect two lines $y = kx + b$ and $y = k'x + b'$, we just have to solve the linear system of two equations in two variables, and we can find (x, y) using arithmetic operations $+, -, \cdot, /$.

From circle, have $(x - x_i)^2 + (y - y_i)^2 = R^2 = (x_j - x_i)^2 + (y_j - y_i)^2$ and compute using $+, -, \cdot$

Intersecting a line and $(x - x_i)^2 + (y - y_i)^2 = R^2$, solve for x, y by substituting the linear equation in for y , and solving the quadratic using the quadratic formula, which requires a square root

Finally, we can intersect two circles $\begin{cases} (x - x_i)^2 + (y - y_i)^2 = R^2 \\ (x - x_j)^2 + (y - y_j)^2 = \overline{R}^2 \end{cases}$ If we subtract, the degree terms go away, and we are left with a linear equation in x and y

Corollary 85. *If α is constructable $\implies \alpha$ is algebraic / \mathbb{Q} , and its degree is a power of 2.*

Proof: $\alpha \in K_r$ like in theorem. Then $[K_r : \mathbb{Q}] = [K_r : K_{r-1}][K_{r-1} : \mathbb{Q}] = 2[K_{r-1} : \mathbb{Q}] = 2^r$ by induction

On the other hand, we have $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K_r$. So again, by transitivity, $2^r = [K_r : \mathbb{Q}] = [K_r : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \implies [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$, which is the degree of the minimal polynomial of α .

Corollary 86. *We can't double the cube.*

Proof: well if we can, then its side, $\sqrt[3]{2}$, is constructable. Therefore, $\sqrt[3]{2}$ has degree 2^s . But it has degree 3, since the minimal polynomial is $x^3 - 2$. Therefore, the cube can't be doubled.

Corollary 87. *We can't trisect a general angle.*

$\cos(\alpha + \beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$. So $\cos(3\phi) = \cos(2\phi)\cos(\phi) - \sin(2\phi)\sin(\phi) = [2\cos^2(\phi) - 1]\cos(\phi) - 2\sin^2(\phi)\cos(\phi) = 2\cos^3\phi - \cos\phi - 2(1 - \cos^2\phi)\cos\phi = 4\cos^3\phi - 3\cos\phi$

Claim: $\cos(60 \deg) = \frac{1}{2}$ is constructable, but $\cos(20 \deg)$ is not. $\cos(20 \deg)$ is a root of $8x^3 - 6x - 1$, which is irreducible. Therefore, the degree of $\cos(20 \deg)$ is 3, which is not a power of 2.

Why irreducible? Well, degree 3, so it has to have a root, and by rational roots theorem it has none in $\{\pm 1, \pm 1/2, \pm 1/4, \pm 1/8\}$, therefore it is irreducible.

Corollary 88. *You cannot square a circle*

If you want to create a square with area π , then you need to construct $\sqrt{\pi}$, which is transcendental / \mathbb{Q} . Suppose $\sqrt{\pi}$ is algebraic / \mathbb{Q} . Then $\sqrt{\pi}\sqrt{\pi}$ must also be algebraic, but in fact π is transcendental (by a difficult theorem proved by Lindemann ~ 1890)

12 FINITE FIELDS

F is a field $\implies F$ contains the smallest possible subfield. This field, known as a prime field, is either \mathbb{Q} or $\mathbb{Z}_p = \mathbb{F}_p$ for prime p

F a finite field $\implies F \supset \mathbb{F}_p$ for $p = \text{char } F \implies F$ is a vector space over $\mathbb{F}_p \implies |F| = p^n$, where $n = [F : \mathbb{F}_p]$

Theorem 89. *There exists a field with p^n elements \forall prime $p, n \geq 1$*

Idea 1: prove existence of an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree $n \implies \mathbb{F}_p[x]/(f) = F$ field with p^n elements. Counting gets harder for $n \geq 2$

Idea 2: let F be a finite field with p^n elements. Then $F^* = F \setminus \{0\}$ is a group with respect to multiplication with $p^n - 1$ elements.

$\implies \forall x \in F^*, \text{ord}(x) | p^n - 1$ (Cauchy theorem)

$\implies x^{p^n - 1} = 1$ in F^*

$\implies x^{p^n} = x \forall x \in F$ (a generalization of Little Fermat Theorem)

Very special polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$ with degree p^n . It's roots are exactly elements of F , $|F| = p^n$

Theorem 90. *Every field F has an algebraic closure, \overline{F} : a field containing F , algebraic over F , and algebraically closed*

Corollary 91. $\mathbb{F}_p \subset \overline{F}$ algebraically closed and algebraic over \mathbb{F}_p

$$x^{p^n} - x \in \mathbb{F}_p[x] = \prod_{i=1}^{p^n} (x - \alpha_i), \alpha_i \in \overline{F}_p$$

Claim: all of these roots are different.

Suppose we can factor $x^{p^n} - x = (x - \alpha_1)^2 g(x) \in \overline{F}_p[x]$. Then take a derivative, $(x^{p^n} - x)' = 2(x - \alpha_1)g(x) + (x - \alpha_1)^2 g'(x)$. But the right side is divisible by $x - \alpha_1$. Well, the left side is $p^n x^{p^n - 1} - 1 = -1$. If we plug in $x = \alpha_1$, we're left with $-1 = 0$, which is obviously a contradiction

Claim: $F = \{a_1, a_2, \dots, a_{p^n}\}$ is a field, so then we have a field with p^n elements.

$F \subset \overline{F}_p$. Now we just have to check closures. Take $x, y \in F$. Then $(xy)^{p^n} = x^{p^n} y^{p^n} \implies xy \in F$

$$(-x)^{p^n} = (-1)^{p^n} x^{p^n} = -x \implies -x \in F$$

$$(x+y)^p = x^p + y^p, (x+y)^{p^2} = [(x+y)^p]^p = (x^p)^p + (y^p)^p = x^{p^2} + y^{p^2}. \text{ By induction, } (x+p)^{p^n} = [(x+y)^{p^{n-1}}]^p = x^{p^n} + y^{p^n}$$

Summary $\mathbb{F}_p \subset F \subset \overline{\mathbb{F}_p}$. $F = \mathbb{F}_{p^n} = \mathbb{F}_q$ where $q = p^n$. Is exactly the set of roots of $x^{p^n} - x \in \mathbb{F}_p[x]$

Theorem 92. Let F be a field with p^n elements $\implies F = \mathbb{F}_p(\alpha)$ for some $\alpha \in F$

Corollary 93. F is isomorphic to $\mathbb{F}_p[x]/(f)$, where (f) is the minimal polynomial of α . In particular, we see that there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$

In fact F^* is cyclic. Take $\alpha \in F^*$ any generator, then $F^* = \{1, \alpha, \alpha^2, \dots, \alpha^{p^n-1}\} \implies F$ is the smallest field that contains $\alpha \implies F = \mathbb{F}(\alpha)$

The proof that \mathbb{Z}_p^* works, because all we used was that the field is finite. If we assume F^* not cyclic, then all elements have order strictly less than $p^n - 1$, but that can't happen since we have $p^n - 1$ roots

Theorem 94. If E and F are finite fields with p^n elements, then they are isomorphic

Proof Write $E = \mathbb{F}_p(\alpha)$ for $\alpha \in F$. $f(x) = \text{irr}(\alpha, \mathbb{F}_p)$ irreducible of degree n . But we know that $\alpha^{p^n} = \alpha \implies \alpha$ is a root of $x^{p^n} - x = 0$, therefore $f(x)$ divides $x^{p^n} - x$.

Now consider F , $|F| = p^n$. $\forall x \in F \implies x^{p^n} - x = 0$. Well, this factors as $f(x)g(x)$. Has p^n roots (all elements of F are roots). So, there exists some element β such that $f(\beta) = 0$ since f has degree n

$\mathbb{F}_p \subset \mathbb{F}_p(\beta) \subset F$. $\deg(\beta) = \deg(f) = n \implies [F : \mathbb{F}_p] = [\mathbb{F}_p(\beta) : \mathbb{F}_p] \implies F = \mathbb{F}_p(\beta)$. So $E = \mathbb{F}_p(\alpha)$ and $F = \mathbb{F}_p(\beta)$, both of which have f as their minimal polynomial. Therefore, $E \cong \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(f) \cong \mathbb{F}_p(\beta) \cong F$

Remark 95. Can it happen that $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$?

Let's consider $F_{p^n}^* \subset F_{p^m}^*$, well the left is a cyclic group of order $p^n - 1$ and the right is a cyclic group of order $p^m - 1$. So we have $p^n - 1 | p^m - 1$

Let's try long division. $p^m - 1 = p^{m-n}(p^n - 1) + p^{m-n} - 1$. Then we need $p^n - 1 | p^{m-n} - 1$

Theorem 96. $p^n - 1$ divides $p^m - 1$ if and only if $n|m$

$$n|m \iff n|m - n \implies \text{Induction on } m \implies p^n - 1 | p^{m-n} - 1 \iff n|m$$

Corollary 97. If $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n|m$

13 GROUP WORK 6

Group 2 Let $ax^2 + bx + c$ be a quadratic equation ($a \neq 0$) with coefficients in a field K with characteristic $\neq 2$.

(1) Show that the usual quadratic formula gives roots of the equation either in K or in some field extension F of K such that $[F : K] = 2$

Proof $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Because $a \neq 0, \text{char}(K) \neq 0$, we know that $2a \neq 0$

Case 1: $b^2 - 4ac = d^2$, ($d \in K$) $x = -\frac{b \pm d}{2a}$, so x is in K

Case 2: $b^2 - 4ac \neq d^2$, take $x^2 - D$ where $D = b^2 - 4ac \in K$, then take the field extension $F(\alpha)$ where $\alpha^2 = D$. Then this is obviously degree two.

(2) Let F be a field extension of K such that $[F : K] = 2$ and $\text{char} K \neq 2$. Show that there exists $D \in K$ such that $F = K(\sqrt{D})$

Proof Let $\beta \in F, \beta \notin K$. We now that $[F : K] = 2$, and $[K(\beta), K] > 1$. Then $[F : K] = [F : K(\beta)][K(\beta) : K] = 2$, so $[F : K(\beta)]$ must be 1, and $F = K(\beta)$

β is the solution to $ax^2 + bx + c = 0$, and $\beta = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-b \pm \sqrt{D}}{2a}$. Therefore, $\sqrt{D} \in K(\beta)$ and $K(\sqrt{D}) \subset K(\beta)$, therefore $K(\beta) = K(\sqrt{D})$. Therefore $F = K(\sqrt{D})$, and we are done.

(3) Show that (1) can fail if $\text{char} K = 2$ **Proof** $[\mathbb{F}_4 : \mathbb{F}_2] = 2$, but both of the elements of \mathbb{F}_2 have square roots, the quadratics are reducible

Group A Let $F \subset K$ be a field extension and let $K_1, K_2 \subset K$ be subfields containing F , Let $K_1 K_2 \subset K$ be the smallest subfield containing K_1 and K_2 Suppose K_1 and K_2 are algebraic over F

(1) Show that $K_1 K_2$ is algebraic over F

Proof Michael was mid proof and Tevelev went "Looks like an orgy of greek letters and summation signs" so we will do it next time

\mathbb{Z} and $k[X]$ where k is a field are principle ideal domains. Both have long division.

Definition 98. An integral domain D is a Euclidean domain if there exists a function (called norm) $v : D \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$, such that for every $a, b \in D$, either $a = bq$ or $a = bq + r$, where $v(r) < v(b)$, and $v(ab) \geq v(a)$

Example. \mathbb{Z} , $v(a) = |a|$

Example. $k[X]$, $v(f) = \text{degree}$

Theorem 99. Every Euclidean domain is a PID [and therefore a UFD]

Take $I \subset D$ ideal. If $I = \{0\} \implies I$ is principal. $I \neq \{0\} \implies$ pick $a \in I$ to be the element of smallest norm.

Claim: $I = (a)$. Take $b \in I$. If $b = aq$, then great. If not, do $b = aq + r$, where r has to have norm less than that norm of a , but $r = b - aq$, both of which are in the ideal, so we've found an element of norm smaller than a , contradiction.

Example. Gaussian Integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$

Forms a grid graphically. This is definitely a commutative ring with 1. $\mathbb{Z}[i] \subset \mathbb{C}$ subring, therefore it must be an integral domain.

Norm: $a^2 + b^2$. Take $\alpha, \beta \in \mathbb{Z}[i]$. Draw $(\beta) = \gamma\beta$ where $\gamma \in \mathbb{Z}[i]$. $\beta(a + bi) = a\beta + ib\beta$. Plot for all a, b

it could be the case that α is already onto the grid. If not, then $\alpha = \beta\gamma + \delta$ where $v(\delta) < v(\beta)$. So choose the square containing α . Chose $\beta\gamma$ to be the vertex of the square that α is closest to. Then $|\delta| < |\beta|$ since β is the side length. But quarter circles cover the square.