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

Definition 7 (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 8. 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 9. 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 10 (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 11 (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. 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. For $R = \mathbb{Z}_n$, $x \in \mathbb{Z}_n$ is a unit $\iff \gcd(x, n) = 1$.

Definition 12. 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 13. *$n = rs$, r, s coprime, $\mathbb{Z} \cong \mathbb{Z}_r \times \mathbb{Z}_s$ (as rings). Implies Chinese Remainder Theorem*

Theorem 14. *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 15. *r, s coprime, $n = rs \implies \mathbb{Z}_n^* \cong \mathbb{Z}_r^* \times \mathbb{Z}_s^*$*

Corollary 16. *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 $1 \le x \le r$ coprime to r and $1 \le y \le s$ coprime to s, and we can use a combinatorial argument to say that there are $\phi(r)\phi(s)$ such pairs.

Corollary 17. *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 18 (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 $A = order(x)$, 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 19. *$\mathbb{Z}_p^*$ 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. 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 $\mathbb{Z}_{\ltimes'}$

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

3 Field of Fractions

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

Remark 20. $\forall q \in \mathbb{Q}$ can be written as $\dfrac{n}{m}, n, m \in \mathbb{Z}$

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

Theorem 21. *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 22. R is a ring, then $R[X] = \{$polynomials in X with coefficients in $R\}$
$= \{a_0 + a_1x + a_2x^2 + \ldots | a_i \in R$, finitely many nonzero $a_i\}$

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

Remark 23. 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 24. $f(x) \in R[X]$. $r \in R$ 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 25 (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 26. *$R[X]$ 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
$(a_0 + a_1x + \ldots)(b_+b_1x + \ldots) = (a_0 + b_0) = (\sum_{i \geq 0} a_ix^i)(\sum_{j \geq 0} b_jx^j) = \sum_{i,j} = a_ib_jx^{ij}$

Remark 27. 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 28. 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 29. Fields are the easiest rings. The next "easiest" ring is $F[X]$, where F is a field

Definition 30 (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 31. 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.*

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

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 32. $\phi : R \to S$ 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 33. 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 34. 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 35. *For any homomorphism $\phi : R \to S$, Kerϕ 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 36. *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 37. 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 38. *$I \subset R$ 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 39. 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 40. 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 41. *$R = F[x]$ 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 42. ϕ is one to one $\iff$ Ker$\phi = \{0\}$

Because this is true for homomorphisms of abelian groups.

Definition 43. 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. 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 44. For $p \in R$ irreducible, if $p = ab \implies a$ or b is a unit

Definition 45. 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 46. If p is prime then p is irreducible

Definition 47. 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 48. 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 $a = up_1 \dots p_{i-1}(\alpha p)p_{i+1} \dots p_r \implies p|a$

Remark 49. 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 $p_1 | vq_1 \ldots q_s$. $p_1 \nmid u \implies p_1 | q_i$ 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: $up_2 \ldots p_r = (v\beta) q_2 \ldots q_s$. 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. $r_1 = r_2 b_2$, b_2 is not a unit. Can continue inducting, and get a sequence $r_i = r_{i+1} b_{i+1}$ where all $r_1, r_2, \ldots$ 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 $r_{i+1} = r_i c_i \implies r_i = r_i b_{i+1} c_i \implies 1 = b_{i+1} c_i \implies b_{i+1}$ is a unit, contradiction.

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

Definition 50. 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 51. *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 52. *$K \to K[x] \to K[x]/I = F \implies K \to F$ by composition. $f(x)$ has a root $\alpha \in F$*

Corollary 53. *If you take any polynomial in $f(x) \in K[x]$, factors into linear factors in some field extension of $K \subset F$*

Proof: $K \xrightarrow{\phi} F$. 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 54. 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 55. 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 56. *e, π are transcendental over $\mathbb{Q}$*

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

Remark 57. 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 58. *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 $irr(\alpha, K)$ 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. $irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, $irr(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$.

Definition 59. 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.

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

Apply the first isomorphism theorem:

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

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

Claim: $Im(\phi) = K(\alpha)$. Why is it the smallest? Suppose N is a subfield of F that contains K and α. Is $Im(\phi) \in N$? 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 $p(x) \to p(\alpha)$. $I = \text{Ker}\phi = 0 \implies \phi$ is injective.

$K[x] \stackrel{\phi}{\to} F \implies K(x) = \{\frac{p(x)}{q(x)} : p, q \in K[x]\}$ 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 60. We can imbed field K into a ring R and this still holds since we used ring axioms only.

Definition 61. 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 62. $v_1, \ldots v_k$ are **linearly independent** if $\sum a_1 v_1 = 0 \implies \forall a_i = 0$.

Definition 63. $\{v_1, \ldots, v_k\}$ is a **basis** if they span and are linearly independent.

Lemma 64. *$v_1, \ldots, v_n$ span V and $u_1, \ldots, u_k$ are linearly independent, then $k \leq n$.*

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

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

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

Corollary 65. *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

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

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

Definition 66. $K \subset F$ 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 67. *$f(x) \in K[x]$ 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, $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{n-1}$ 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 $r <$ degree 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 $a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + I, a_i \in K$ uniquely. $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = a_0(1+I) + a_1(x+I) + \ldots + a_{n-1}(x+I)^{n-1} =$ above.

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

Corollary 68. *$K \subset F$ field extension, $\alpha \in F$ algebraic over K with minimal polynomial of degree $n \implies [K(\alpha), K] = n$, with basis $\{1, \alpha, \ldots, \alpha^{n-1}$.*

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

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

$\mathbb{Q}(\sqrt{2}), irr(\sqrt{2}) = x^2 - 2 \implies [Q(\sqrt{2}), \mathbb{Q}] = 2$, 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 $\dfrac{1}{1 + \alpha + \alpha^2}$ as linear combination?

$x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3$, solve for $x_0, \ldots x_4$. $1 = (1 + \alpha + \alpha^2)(x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3)$. $\alpha^4 = 2\alpha^2 + 2$. 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 69. A field extension $K \subset F$ is called **algebraic** if every element $\alpha \in F$ is algebraic$/K$.

Theorem 70. *Every finite extension is algebraic*

$[F : K] = n, \alpha \in F$. Basis $e_1, e_2, \ldots, e_n \in F$. Take $1, \alpha, \ldots, \alpha^n$. Are linearly dependent $\implies x_0 + x_1\alpha + \ldots + x_n\alpha^n = 0$ 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 71. 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 $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, where n is the degree of $f(x) = [F(\alpha) : F]$

Theorem 72 (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 $\alpha_1, \ldots, \alpha_n$ of K as a vector space over F. Choose $\beta_1, \ldots, \beta_m$ of L as a vector space over K. Claim $\alpha_i\beta_j$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ 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 73. *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 $\implies \deg(irr(\beta, \mathbb{Q})) = [\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$

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 polynommial 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 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 $F \subset K$ i algebraic $\implies L = K$.

Lemma 74. *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 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 75. How can we find a

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

Definition 76. 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) $a + bi \in C$ 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. $c = \sum_{n\geq 1} \frac{1}{10^{n!}}$

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 77. *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/$\mathbb{Q}$

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

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

Choose $\frac{p}{q}$ such that $\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^n}$. Then $f(\alpha) - f(\frac{p}{q}) = f'(x)(\alpha - \frac{p}{q})$ 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 $\sup\limits_{|x-\alpha| \leq 1} |f'(x)|$, 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 $1 \to \mathbb{Q}$. 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 78. $\alpha \in \mathbb{R}$ *is constructible* $\iff$ *there exists* $\mathbb{Q} = K_0 \subset K_1 \subset K_r$ *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 arithimetic 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 79. *If α is constructable $\implies$ α is algebraic / $\mathbb{Q}$, and its degree is a power of 2.*

Proof: $\alpha \in K_r$ like in theorem. Then $[K_r : Q] = [K_r : K_{r-1}][K_{r-1} : \mathbb{Q}] = 2[K_{r-1} : \mathbb{Q}] = 2^r$ 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 80. *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 81. *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 82. *You cannot square a circle*

If you want to create 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 $\sim$ 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 $p = charF \implies F$ is a vector space over $\mathbb{F}_p \implies |F| = p^n$, where $n = [F : \mathbb{F}_p]$

Theorem 83. *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 multiplcation 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 84. *Every field F has an algebraic closure, $\overline{F}$: a field containing F, algebraic over F, and algebraically closed*

Corollary 85. *$\mathbb{F}_p \subset \overline{F}$ 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, $(x^{p^n} - x)' = 2(x-\alpha_1)g(x) + (x-\alpha)^2 g'(x)$. 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: $F = \{a_1, a_2, \ldots, a_{p^n}\}$ is a field, so then we have a field with p^n elements.

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

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

$(x+y)^p = x^p + y^p$, $(x+y)^{p^2} = [(x+y)^p]^p = (x^p)^p + (y^p)^p = x^{p^2} + y^{p^2}$. 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 86. *Let F be a field with p^n elements $\implies F = \mathbb{F}_p(\alpha)$ for some $\alpha \in F$*

Corollary 87. *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 $F^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{p^n-1}\} \implies F$ 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 88. *If E and F are finite fields with p^n elements, then they are isomorphic*

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

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

$\mathbb{F}_p \subset \mathbb{F}_p(\beta) \subset F$. $\deg(\beta) = deg(f) = n \implies [F : \mathbb{F}_p] = [\mathbb{F}(\beta) : \mathbb{F}_p] \implies F = \mathbb{F}_p(\beta)$. 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 89. Can it happen that $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$?

Let's consider $F_{p^n}* \subset \mathbb{F}_{p^m}^*$, 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 90. *$p^n - 1$ divides $p^m - 1$ if and only if $n|m$*

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

Corollary 91. *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 $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Because $a \neq 0, char(K) \neq 0$, we know that $2a \neq 0$

Case 1: $b^2 - 4ac = d^2, (d \in K)$ $x = -\dfrac{-b \pm d}{2a}$, 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 $charK \neq 2$. 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 $\beta = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \dfrac{-b \pm \sqrt{D}}{2a}$. 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 $charK = 2$ **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 $K_1K_2 \subset K$ be the smallest subfield containing K_1 and K_2 Suppose K_1 and K_2 are algebraic over F

(1) Show that K_1K_2 is algebraic over F

14 Euclidean Domains

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

Definition 92. An integral domain D is a Euclidean domain if there exists a function (called norm) $v : D \setminus \{0\} \to \mathbb{Z}_{\geq 0}$, 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. $k[X]$, $v(f) =$ degree

Theorem 93. *Every Eucliean 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 r, 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.

Theorem 94. *A PID is a UFD*

Proof we need to prove existence and uniqueness of factorization: $\alpha = u\beta_1 \cdots \beta_n$, with u unit and β_i irreducible.

Existence: suppose that there is some α without factorization. Then it cannot be a unit, and it is not irreducible. Then $\alpha = \beta\gamma$ where neither β nor γ is a unit. If both are factorable, we win, and multiply their factorizations. If not, then say β is not factorable. Then take this chain of $\alpha_i = \alpha_{i+1}\gamma_{i+1}$. $(\alpha_1) \subsetneq (\alpha_2)$. If they are equal, then γ must be a unit, since $\alpha_1 = \alpha_2\gamma_2, \alpha_2 = \alpha_1\gamma_1, \alpha_1 = \alpha_1\gamma_1\gamma_2 \implies \gamma_1\gamma_2 = 1$ units.

So now we have $(\alpha_1) \subsetneq (\alpha_2) \subsetneq (\alpha_3) \subsetneq \ldots$. Take the union $I = \cup_{i \geq 1}(\alpha_i)$. Usually not an ideal, but in this case it is. Take two elements in it $x, y \in I$. $x \in (\alpha_i), y \in (\alpha_j)$, but are both in one of the ideals.

I ideal, generated by something since PID, z, then $(\alpha_i) \subsetneq I \subset (\alpha_i)$ contradiction

Uniqueness of factorization $u\beta_1 \dots \beta_r = u'\beta_1' \dots \beta_r'$. β_1 divides the left hand side, so it divides the righthand side. Can't be u' since it's a unit. $\beta_1' \in (\beta_1) \implies \beta_1' = \beta_1 t$, both β are irreducible so t must be a unit, and are associate. We induct over the irreducibles, and get all of our associate pairs.

Lemma 95. *$\beta \in R$ β irreducible, R PID, then (β) is prime*

$\beta \in R$ is prime $\iff$ $R/(\beta)$ is an integral domain. Not only that, but in our case, it is a field $\iff$ (β) is a maximal ideal, since $(\beta) \subset I \subset R \implies (\beta) \subset (\gamma) \subset R$, but then $\beta = \gamma\delta$, so (γ) is either (β) or R

Back to $\mathbb{Z}[i]$. Units are $\pm 1, \pm i$. Otherwise, $\alpha\beta = 1$, so the norms multiply to one, so norm of α must be 1 since it must be an integer. Then $\alpha = a + bi$, $\text{norm}(\alpha) = a^2 + b^2$, so $\alpha = \pm 1, \pm i$

Irreducible elements in $\mathbb{Z}[i]$?
Claim: $\alpha \in \mathbb{Z}[i], N(\alpha) = p$ prime $\implies$ α is irreducible.

Indeed, suppose that $\alpha = \beta\gamma$. Then $N(\alpha) = N(\beta)N(\gamma) = p$, so by Euclid's lemma one must be 1, so therefore must be a unit.

Theorem 96 (Fermat)**.** *Odd prime $p \in \mathbb{Z}$ can be written as the sum of two squares $\iff$ $p \equiv 1 \pmod 4$*

Left to right is easy, since $a^2 + b^2$ each term is either 0, 1, so the sum can only be 0, 1, 2, but p is odd, so must be one.

Take $p \equiv 1 \pmod 4$. $\mathbb{Z}_p^*$ is a cyclic group of order $p - 1 = 4k$. Therefore, there must be an element of order 4, call it x. Then x^2 has order 2. But then x^2 must be congruent to -1 mod p. Then there is $x \in \mathbb{Z}$ such that $p | x^2 + 1$.

Over $\mathbb{Z}[i]$, we have $x^2 + 1 = (x + i)(x - i)$, so $p|(x + i)(x - i)$. Can it happen that p is irreducible over $\mathbb{Z}[i]$

Suppose that p is irreducible. Then p divides the product in a UFD, so it must divide one of the divisors. $p|(x + i)$ or $p|(x - i)$. Then $x = pa$ and $1 = pb$, contradiction. Therefore, p is not an irreducible Gaussian integer, so $p = \alpha\beta$ not units. $\implies N(p) = N(\alpha)N(\beta) \implies p^2 \implies N(\alpha) = p$, so $a^2 + b^2 = p$

15 Galois Theory

Relationship between algebraic equations, groups, and fields.

Fix $F \subset \overline{F}$, field with algebraic closure. We want to study all possible extensions between F and $\overline{F}$

It can happen that $K \neq L$, but $K \cong L$. It can happen that $\exists f : E \to E$ where $f \neq Id$

Main tool: $K = F(\alpha), \alpha \in \overline{F}$. Take $p(x) = irr(\alpha, F) \in F[x]$, then $F[x]/(p) \xrightarrow{isom.} F(\alpha)$, $x + (p) \mapsto \alpha$. In particular, every $\gamma \in F(\alpha)$ can be written uniquely as $a_0 + a_1\alpha + a_2\alpha^2 + \dots a_{n-1}\alpha^{n-1}$, $a)i \in F$, $n = degp(x) = [F(\alpha) : F]$

Definition 97. α, β are called conjugate if $irr(\alpha, F) = irr(\beta, F)$. Equivalently α and β are roots of the same irreducible polynomial in $F[x]$

Corollary 98. *If α and β are conjugate, then $F(\alpha) \cong F(\beta)$ with $a_0 + a_1\alpha + \dots a_{n-1}\alpha^{n-1} \mapsto a_0 + a_1\beta + \dots + a^{n-1}\beta^{n-1}$*

Proof Both are isomorphic to $F[x]/(p)$, so

Example. $\mathbb{Q} \subset \overline{\mathbb{Q}}$

$p(x) = x^2 - 2 \in \mathbb{Q}[x]$ irr. $\implies$ $\sqrt{2}$ is conjugate to $-\sqrt{2}$ over $\mathbb{Q}$. Therefore there is an isomorphism from $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(-\sqrt{2})$ where $a + b\sqrt{2} \mapsto a - b\sqrt{2}$

$K = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$, therefore K has a nontrivial automorphism.

Example. $p(x) = x^3 - 2$ irreducible over $\mathbb{Q}$, $\alpha = \sqrt[3]{2}$, $\beta = \sqrt[3]{2}e^{2\pi/3}$

Therefore, $\mathbb{Q}(\alpha) \xrightarrow{\sim} \mathbb{Q}(\beta)$ sends $a_0 + a_1\alpha + a_2\alpha^2 \mapsto a_0 + a_1\beta + a_2\beta^2$. However, they cannot possibly be the same field, since one has only real numbers, whereas the second obviously contains β, but $\beta \notin \mathbb{R}, \beta \in \mathbb{C}$

Example. $F = \mathbb{R} \subset \overline{\mathbb{R}} = \mathbb{C}$

$[\mathbb{C} : \mathbb{R}] = 2$, so there cannot be any intermediate fields. If we take i, which is a root of $x^2 + 1 \in \mathbb{R}[x]$ irreducible/$\mathbb{R}$, as is $-i$. Then we have two conjugate elements, so we have an isomorphism from $\mathbb{R}(i) \xrightarrow{\sim} \mathbb{R}(-i)$ sending $a + bi \mapsto a - bi$ $\implies$ we get an automorphism of $\mathbb{C}$, $a + bi \mapsto a - bi$ called complex conjugation

Example. Take $F = \mathbb{F}_2 \subset \mathbb{F}_4 \subset \overline{\mathbb{F}}_2$. Choose $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$

$irr(\alpha, \mathbb{F}_2) = x^2 + x + 1$, the unique irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$

Another element in $\mathbb{F}_4 \setminus \mathbb{F}_2$: $\alpha + 1$ (if $\alpha + 1 \in \mathbb{F}_2 \implies \alpha = \alpha + 1 + 1 \in \mathbb{F}_2$)

$irr(\alpha + 1, \mathbb{F}_2) = x^2 + x + 1 \implies \exists$ an isomorphism $\mathbb{F}_2(\alpha) \xrightarrow{\sim} \mathbb{F}_2(\alpha + 1)$ $a + b\alpha \mapsto a + b(1 + \alpha) = a + b\alpha^2$, since $\alpha + 1 = \alpha^2$, so $a + b\alpha \mapsto a + b\alpha^2 = (a + b\alpha)^2$, the Frobenius homomorphism $\mathbb{F}_4 \to \mathbb{F}_4$, $x \mapsto x^2$.

Example. $F = \mathbb{Q}(\sqrt{2})$, $\sqrt{4} \notin \mathbb{Q}(\sqrt{2})$ since $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2}) \implies \sqrt{3}$ and $-\sqrt{3}$ are conjugate over both $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$.

$\implies \mathbb{Q}(\sqrt{2})(\sqrt{3}) \to \mathbb{Q}(\sqrt{2})(-\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$, sends $a + b\sqrt{3} \mapsto a - b\sqrt{3}$ for $a, b \in \mathbb{Q}(\sqrt{2})$

Then we can write $a = c + d\sqrt{2}$, $c, d, \in \mathbb{Q}$, and $b = e + f\sqrt{2}$, $e, f \in \mathbb{Q}$, so $c + d\sqrt{2} + e\sqrt{3} + f\sqrt{6} \mapsto c + d\sqrt{2} - e\sqrt{3} - f\sqrt{6}$

So $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has a basis $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ over $\mathbb{Q}$ and an automorphism

$$\sigma: \quad \begin{aligned} 1 &\mapsto 1 \\ \sqrt{2} &\mapsto \sqrt{2} \\ \sqrt{3} &\mapsto -\sqrt{3} \\ \sqrt{6} &\mapsto -\sqrt{6} \end{aligned}.$$

Analogusly, it has an automorphism

$$\tau: \quad \begin{aligned} 1 &\mapsto 1 \\ \sqrt{2} &\mapsto -\sqrt{2} \\ \sqrt{3} &\mapsto \sqrt{3} \\ \sqrt{6} &\mapsto -\sqrt{6} \end{aligned}$$

$\sigma^2 = \tau^2 = Id$, but

$$\tau \circ \sigma: \quad \begin{aligned} 1 &\mapsto 1 \\ \sqrt{2} &\mapsto -\sqrt{2} \\ \sqrt{3} &\mapsto -\sqrt{3} \\ \sqrt{6} &\mapsto \sqrt{6} \end{aligned}$$

$\implies \{1, \sigma, \tau, \sigma\tau\}$ is a group of automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, K_4

Remark 99. $Aut(K)$ is a group with respect to composition.

Definition 100. $\sigma_1, \ldots, \sigma_r \in \operatorname{Aut} K$. $K^{\{\sigma_1, \ldots, \sigma_r\}} = \{x \in K : \sigma_i(x) = x \forall \sigma_i\}$

Example. $\mathbb{Q}(\sqrt{2}, \sqrt{3})^\sigma = \{a + b\sqrt{2}\} = \mathbb{Q}(\sqrt{2})$. $\mathbb{Q}(\sqrt{2}, \sqrt{3})^\tau = \mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\sigma\tau} = \mathbb{Q}(\sqrt{6})$, and $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\{\sigma, \tau\}} = \mathbb{Q}$

Lemma 101. *$K^{\sigma_1, \ldots, \sigma_r}$ is a subfield of K*

Proof just the regular field tests for all elements

Given a subgroup $H \subset \operatorname{Aut} K$, field $K^H \subset K$ is the field of all elements fixed by H, $\{x \in K | \sigma(x) = x \forall \sigma \in H\}$

Definition 102. Take fields $L \subset K$. Then $G(K/L) = \{\sigma \in \operatorname{Aut} K : \sigma(x) = x \forall x \in L\}$

Lemma 103. *$G(K/L)$ is a subgroup of* $\operatorname{Aut}(K)$

Proof σ, $\tau \in G(K/L)$. Compute $\sigma\tau(x) = \sigma(x) = x$ for $x \in L$. Also, $\sigma(x) = x \implies x = \sigma^{-1}(x) \implies \sigma^{-1} \in G(K/L) \implies G(K/L)$ is a subgroup by the subgroup test

How do we understand isomorphisms $\sigma : K \to L$?

Fact If σ is an isomorphism $K \to L$ that fixes every element of $F \implies \alpha$ and $\sigma(\alpha)$ are conjugate.

Proof $p(x) = irr(\alpha, F)$. Then $p(\alpha) = 0$. Now just apply $\sigma(p(\alpha)) = 0$. Use automorphism $\implies$ homomorphism $\implies \sigma(p(x)) = \sigma(a_0) + \sigma(a_1\alpha) + \ldots + \sigma(a_{n-1}\alpha^{n-1}) = a_0 + a_1\sigma(\alpha) + \ldots + a_{n-1}\sigma(\alpha)^{n-1} = 0$. (Important that $\sigma(a_i)$ $= a_i$ since σ fixes elements of F)