algebraic number: α is a root of polynomial

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad a_i \in \mathbb{Q},\ a_0 \neq 0.$$

algebraic integer: root of polynomial

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0. \quad b_i \in \mathbb{Z}.$$

E.g. A rational number $r \in \mathbb{Q}$ is an alg. int. $\iff r \in \mathbb{Z}$.

($\Leftarrow$) $x - r = 0$. ✓.

($\Rightarrow$) suppose $r = \frac{c}{d}$, $\gcd(c,d) = 1$.

with $\left(\frac{c}{d}\right)^n + b_1\left(\frac{c}{d}\right)^{n-1} + \cdots + b_n = 0$ $\quad * d^n$ to clear denoms.

$\Rightarrow \quad c^n + b_1 c^{n-1} d + \cdots + b_n d^n = 0$ so, in part.

must be $\equiv 0 \pmod d$ $\Rightarrow d \mid c^n \Rightarrow \gcd(d,c) > 1$ unless $d = \pm 1$. ↯.

In order to determine
if we can perform modular arithmetic, must see if resulting sets form a ring.

—

$\mathbb{Q}$-module: finite dimensional vector space V over $\mathbb{Q}$.

(I) $a + b \in V$, if $a, b \in V$

(II) if $a \in V$, $r \in \mathbb{Q}$, $r \cdot a \in V$

(III) $\exists$ finite list $v_1, \ldots, v_n \in V$ s.t.

any $v \in V$ written $v = \sum_{i=1}^{n} r_i \cdot v_i$, some $r_i \in \mathbb{Q}$

Prove that set of alg. #'s forms a field. / alg. ints. forms a ring.

—

(a little tricky, use characterization : linear algebra: given $\mathbb{Q}$-vector space gens. $\gamma_1, \dots, \gamma_\ell \in \mathbb{C}$ call it V.

then $\alpha\gamma \in V$ for all $\gamma \in V$

$\Rightarrow$ α algebraic (expression involving dets. $= 0$))

Show that property is preserved under addition / mult.

- similar idea w/ $\mathbb{Z}$-mods. for alg. ints.

—

α : alg. #, then α : root of unique monic irred. $f(x) \in \mathbb{Q}[x]$.

(if $g(x) \in \mathbb{Q}[x]$, w/ $g(\alpha) = 0$ then $f(x) \mid g(x)$)

Easy: choose $f(x)$: poly. of smallest degree s.t. $f(\alpha) = 0$.

use Euclidean alg. for polynomials.

—

Any subfield $F/\mathbb{Q} \subseteq \mathbb{C}$ with $[F:\mathbb{Q}]$ finite

"alg. # field"

and set of alg. ints in F : ring of alg. ints. : R.

e.g. $\sqrt{-3}$. / ω. generate $\mathbb{Q}[\omega] = \mathbb{Q}[\sqrt{-3}]$.

plan for higher reciprocity laws: attach ζ_n to $\mathbb{Z}$.

e.g. $n =$ ~~[illegible]~~ 5. $\quad x^5-1 = (x-1)(\underbrace{x^4+x^3+x^2+x+1}_{})$

this is minimal polynomial.

there is a norm map on this ring.

Write basis for $F/\mathbb{Q}$. Express $\alpha\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j$
$\alpha_1, \dots, \alpha_n$

write down a matrix (a_{ij}). $\quad N(\alpha) = \det(a_{ij})$

(also $t(\alpha) = \text{trace}(a_{ij})$ additively inv.)

—

e.g. $\mathbb{Q}[\omega]$. basis: $1, \omega$.

$N(a+b\omega)$: $(a+b\omega)\cdot 1$

$$\begin{pmatrix} a & b \\ -b & a-b \end{pmatrix}$$

$(a+b\omega)\,\omega$

mult., indep. of choice of basis.

$\det(\cdot) = a^2-ab+b^2$. ✓.

$= a\omega + b\omega^2$

$= a\omega + b(-1-\omega)$

$= -b + (a-b)\omega$

- unique factorization?
- definition of ideal: $I \subseteq R$ with $a,b \in I \Rightarrow a+b \in I$, $r \in R, a \in I \Rightarrow ra \in I$.

  what are the ideals of $\mathbb{Z}$?

- P.I.D. $\Rightarrow$ unique factorization.

  ($\Leftarrow$) FALSE (polynomials in >1 var. over field)

Stark's List:

$-1, -2, -3, -7, -11$
$-19, -43, -67$
-163

ideal : $A \subseteq R$: set with $a, b \in A \Rightarrow a+b \in A$

$a \in A$, $r \in R \Rightarrow r \cdot a \in A$.

examples : (n) : ideal generated by n, $\in \mathbb{Z}$. : all int. mults.

Do this in any ring. $(\alpha) \in R$.

Also consider $(\alpha_1, \dots, \alpha_m) \in R$. (smallest ideal containing all these elts.)

in $\mathbb{Z}$, $(4,6) = (2)$, $(m,n) = (\gcd(m,n))$.

in fact, all ideals in $\mathbb{Z}$ are principal.

FACT : if R Euclidean, then R is P.I.D. (so same true for $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$.)

(and every non-zero, non-unit, can be factored as a (unique) product of irreducibles)

But we know that we don't always have unique factorization.

e.g. $\mathbb{Z}[\sqrt{-5}]$. $6 = 2 \cdot 3 = (1-\sqrt{-5})(1+\sqrt{-5})$

so must not be a P.I.D. $(2, 1+\sqrt{-5})$ is non-principal ideal.

prime ideal : if $ab \in P$, then either $a \in P$ or $b \in P$; product of ideals.

Two quick facts about ideals:

FACT 1: For $\beta \in F$, $\exists$ $b \in \mathbb{Z}$, $b \neq 0$, s.t. $b \cdot \beta \in R$.

pf : $\exists$ $f(x)$ with $f(\beta) = 0$. Write $a_0(\beta)^n + \dots + a_n = 0$, $a_0 \neq 0$.

mult. by a_0^{n-1}, write $(a_0\beta)^n + \dots + a_n a_0^{n-1} = 0 \Rightarrow a_0\beta$ is alg. int. //

since $a_0^{i-1} \cdot a_i \in \mathbb{Z}$.

FACT 2 : Every ideal $A \subseteq R$ contains a basis for $F/\mathbb{Q}$.

pf of FACT 2: Let $\beta_1, \dots, \beta_n$: basis for $F/\mathbb{Q}$. Know $\exists$ $b \in \mathbb{Z}$

s.t. $b\cdot\beta_1, \dots, b\cdot\beta_n \in R$. Given $\alpha \in A$, $\alpha \neq 0$, then

elts. $b\cdot\beta_1\alpha, \dots, b\cdot\beta_n\alpha$ are all in A, and a basis for $F/\mathbb{Q}$.

Prop: $A \subseteq R$, ideal. , $\alpha_1, \dots, \alpha_n \in A$. Basis for $F/\mathbb{Q}$ with

$|\Delta(\alpha_1, \dots, \alpha_n)|$ minimal. Then $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.

—

Given $\alpha_1, \dots, \alpha_n$ with $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$, say $\alpha_1, \dots, \alpha_n$ is

basis for $F/\mathbb{Q}$ an "integral basis"

Lemma: if $A \subseteq R$, ideal, $A \cap \mathbb{Z} \neq \phi$.

pf: Pick $\alpha \in A$, $\alpha \neq 0$. then $\exists$ $f(x)$, monic with $f(\alpha) = 0$.

Write $\alpha^m + \cdots + a_{m-1}\alpha + a_m = 0$ with $a_i \in \mathbb{Z}$. , we may

assume $a_m \neq 0$. so then $a_m \in A$. //

Proposition: For any ideal $A \subseteq R$, R/A is finite.

pf: Given $a \in A \cap \mathbb{Z}$, $a \neq 0$, then $(a) \subseteq A$ so

there is a surjective map $R/(a) \to R/A$. So enough to show

$D/(a)$ finite. Check that $S = \{ \sum \gamma_i w_i \mid 0 \leq \gamma_i < a \}$ are

coset reps. with $w_1, \dots, w_n$ a basis.

corollary: # of ideals containing any integer is finite.

Introduce equivalence $\sim$ up to prin. ideals.

since $R/(a)$ finite, so if $(a) \subsetneq A$, then $|R/A| \lneq |R/(a)|$

Lemma: $\exists\ M > 0$, depending only on number field F s.t.:

Given $\alpha, \beta \in R$, $\beta \neq 0$. $\exists\ t$ with $1 \le t \le M$, $w \in R$

s.t. $|N(t\alpha - w\beta)| < |N(\beta)|$. (Euclidean algorithm for arbitrary number field)

pf: Equivalently write $\gamma = \dfrac{\alpha}{\beta} \in F$,

suffices to show that, $\forall\ \gamma \in F$, $\exists\ M$ s.t.

$$|N(t \cdot \underbrace{\tfrac{\alpha}{\beta}}_{\gamma} - w)| < 1. \qquad t \in [1, M].$$

pick integral basis $w_1, \dots, w_n$ for R. For $\gamma \in F$, write

define

$$\gamma = \sum_{i=1}^{n} c_i w_i, \quad c_i \in \mathbb{Q}.$$ Note then that

$$|N(\gamma)| = \left| \prod_j \left(\sum_i \gamma_i w_i^{(j)} \right) \right| \le C \cdot \left(\max_i |\gamma_i| \right)^n$$

with $C = \prod_j \left(\sum_i |w_i^{(j)}| \right)$. Pick $m > \sqrt[n]{C}$,

and take $M = m^n$.

For any $\gamma \in F$, $\gamma = \sum_{i=1}^{n} \gamma_i w_i$ with $\gamma_i = a_i + b_i$ $a_i \in \mathbb{Z}$, $b_i \in [0,1)$

Call $[\gamma] = \sum_{i=1}^{n} a_i w_i$, $\{\gamma\} = \sum_{i=1}^{n} b_i w_i$

Consider $\phi : F \longrightarrow \mathbb{R}^n$ then $\phi(\{\gamma\})$ is in unit cube $[0,1)^n$.

$$\sum_{i=1}^{n} \gamma_i w_i \longmapsto (\gamma_1, \dots, \gamma_n)$$

We can partition the unit cube into m^n subcubes, of side length $1/m$.

Consider the set $\phi(\{k\gamma\})$ for $1 \le k \le m^n + 1$. Know - by pigeonhole principle that two of these are in same subcube, say k_1, k_2 (w.l.o.g. $k_1 > k_2$)

Then
$$k_1\gamma - k_2\gamma = \underbrace{(k_1 - k_2)}_{= t}\gamma = \underbrace{[k_1\gamma] - [k_2\gamma]}_{\in R,\ \text{call it } \omega} + \underbrace{\delta}_{= \{k_1\gamma\} - \{k_2\gamma\}}$$

and coordinates of δ have abs. value $\le 1/m$.

Hence $N(\delta) \le c \cdot (1/m)^n = c/m^n < 1$. ✓.

<u>Thm</u>: class number of F is finite.

<u>pf</u>: A: ideal in R. Choose $\beta \in A$, $\beta \ne 0$, so that $|N(\beta)|$ minimal.

By previous lemma, for any $\alpha \in A$, $\exists\ t$, with $1 \le t \le M$ s.t.

$|N(t\alpha - \omega\beta)| < |N(\beta)|$ with $\omega \in R$. But then $\alpha, \beta \in A \Rightarrow$

$t\alpha - \omega\beta \in A \Rightarrow t\alpha - \omega\beta = 0$ (else contradict min. of $|N(\beta)|$.)

$\Rightarrow (M!) \cdot A \subseteq (\beta)$ (<u>idea</u>: some t works for any α.)

Now let $B \overset{\text{def}}{=} (1/\beta)\, M! \cdot A$: ideal in R, $(M!) \cdot A = (\beta) \cdot B$

so since $\beta \in A$, $M!\beta \in (\beta) \cdot B$, $\Rightarrow M! \in B$.

<u>Claim</u>: $M!$ can be contained in at most finitely many ideals.

$\Rightarrow A \sim B$, B one of at most finitely many ideals.

$\Rightarrow h_F$ finite.