Algebraic Number Theory - Semester 2, 2017.

Bas Edixhoven.

Literature.

P. Samuel - Théorie algébrique des nombres

Milnor + Husemoller - Symmetric bilinear forms.

JWS Cassels + Fröhlich

Serge Lang. Alg. no. thy.

" " Algebra.

Borevich + Shafarevich : Alg. no. thy.

Bourbaki - Algèbre commutative.

group
lds

Introduction. Number theory is the study of integers; many statements about them are easy to state but difficult to prove; eg. Fermat & Goldbach's conjecture. Throughout history, number theory has been a source of delight & despair; it involves most of the branches of mathematics: analysis, algebra, rep theory, topological groups, etc. In some ways, no. thy. is a unifying subject. | 2 major breakthroughs: Fermat $\Delta P \subset \mathbb{P}$. Recently

Not surprisingly, there are many different viewpoints: one could give two disjoint courses on the subject. Our approach fits well into the "algebraic geometry" viewpoint.

It is in no. thy that the term "ideal" which is fundamental to ring theory & hence in many branches of mathematics arose (Kummer invented "ideal numbers", which are nothing but ideals, in an attempt to prove Fermat).

Other concepts, such as automorphic forms, theta functions, etc. were born in number theory and grew up to have an independent existence.

This course is intended to be an introduction to some of the beautiful results in number theory, to introduce some of the algebraic & geometric techniques which are involved and to indicate some interplay between no. thy & the branches of mathematics.

No. theory is about integers, but already Gauss understood well that to understand $\mathbb{N} = \{0, 1, 2, \dots\}$ one needs to study more general types of integers; the "Gaussian integers" $\{n + im \mid m, n \in \mathbb{Z}\}$ have properties like $\mathbb{Z}$. Other similar rings of integers do not.

Assumed knowledge

(a) Theory of PID's & modules over PID's. (eg. f.g. abelian groups)
(b) Field theory - algebraic extensions, etc; roots of unity, finite fields
(c) Galois extensions & Galois groups.
(d) Elementary module theory.

[I will repeat some of these, but quickly].

Do: (i) algebraic element – degree
(ii) minimal polynomial
(iii) algebraic extension – degree $[E:F]$
(iv) algebraic, transcendental.
(v) conjugates

0. Preliminaries – field extensions.

(0.1) Algebraic field extensions.

Let $F \subseteq E$ be fields – say E is an extension field of F.
The element $a \in E$ is algebraic over F if $\exists f \in F[x]$ such that $f(a) = 0$. Here $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ has degree n if $a_n \neq 0$, and has smaller n.

The set $I(a) = \{ f \in F[x] \mid f(a) = 0 \}$ is clearly an ideal. Moreover $I(a)$ is a prime ideal because if $fg \in I(a)$, then $f(a)\,g(a) = 0$, so $f(a) = 0$ or $g(a) = 0$ & hence $f \in I(a)$ or $g \in I(a)$.

Since $F[x]$ is a PID $I(a) = \langle m(x) \rangle$ where $m(x)$ is uniquely determined up to multiplication by a constant in F; $m(x)$ is the minimal polynomial of $a \in E$; it is irreducible, and any $f \in F[x]$ such that $f(a) = 0$ is a multiple of $m(x)$. eg $\mathbb{C} = \mathbb{R}(i) \cong \frac{\mathbb{R}[x]}{\langle x^2+1 \rangle}$

$F(a) \cong \frac{F[x]}{\langle m(x) \rangle}$

$E \supseteq F$ is an algebraic extension if every elt $a \in E$ is algebraic over F.

$E \supseteq F$ is a finite extension if $\dim_F E < \infty$.

(0.2) Separable extensions.

Suppose $f(x) \in F[x]$, irreducible. Define $Df = \frac{df}{dx}$.
Then
- $f(x)$ has repeated root in some extension $\iff f(x), Df(x)$ have a common root $\iff \gcd(f(x), Df(x)) \neq$ const.
  $\iff$ ideal $\langle f(x), Df(x) \rangle \neq F[x]$.
- Suppose f is irreducible. Then $\langle f(x), Df(x) \rangle = \begin{cases} F[x] & \text{if } Df \neq 0 \\ \langle f(x) \rangle & \text{if } Df = 0 \end{cases}$

Hence: an irred polynomial has repeated roots $(\Rightarrow)$. $Df(x) = 0$.
$\Leftrightarrow f(x) = f_1(x^p)$, where $f_1 \neq 0 \in F[x]$, and
$p = \mathrm{char}(F)$.

Example. Let F have char p and suppose $E \supsetneq F$. If $\theta \in E \setminus F$, then $x^p - \theta$ is irreducible, and in some extension,
$x^p - \theta = (x - \theta_1)^p$ (p odd). $(\theta = \theta_1^p)$.

Def An irred polynomial $f(x) \in F[x]$ is separable if it has distinct roots in some (hence any) extension; otherwise f is inseparable.
f inseparable $\Rightarrow \mathrm{char}\, F = p > 0$.

An element $a \in E \supseteq F$ is separable if its min poly is separable.
Otherwise inseparable.
$E \supseteq F$ is a separable extension if each elt $a \in E$ is separable

The field F is perfect if every algebraic extension is separable
$\mathrm{char}\, F = 0 \Rightarrow F$ is perfect.
F alg closed $\Rightarrow F$ is perfect.
F finite $\Rightarrow F$ is perfect.

Exercise: [Lemma: F perfect $(\Leftrightarrow)$ each elt of F has a p^{th} root ($p = \mathrm{char}\, F$) in F.]
F finite $\Rightarrow a^{p^n} = a$ $\forall a$ — i.e. each elt is a p^{th} power.

Example. $\mathbb{F}_p(z)$ is a field of char p (z indet).
$E = \mathbb{F}_p(z^{\frac{1}{p}}) \supseteq F$ is inseparable.

E_1

Theorem (Thm of the primitive element). Let $F(\alpha_1, \cdots, \alpha_n)$ be a finite extension of F, with $\alpha_2, \cdots, \alpha_n$ separable over F. [each α_i is algebraic]. Then $\exists\, \theta$ s.t. $F(\alpha_1, \cdots, \alpha_r) = F(\theta)$.

Proof We may assume F is infinite, for if F is finite, $E \cong \mathbb{F}_{p^N}$ and $\mathbb{F}_{p^N}^*$ is a finite cyclic group, with generator θ, so $E = F(\theta)$. So we assume F is infinite. Wlog we may take $n = 2$, ie $E = F(\alpha, \beta)$ with β separable.

Let $f(x), g(x)$ be the minimal polynomials of α, β resp over F; let the roots of f be $\alpha = \alpha_1, \cdots, \alpha_r$, & $\beta = \beta_1, \cdots, \beta_s$ respectively.

Since F is infinite, $\exists\, c \in F$ s.t. $(\alpha_i - \alpha) + c(\beta_j - \beta) \neq 0 \;\forall\, i, j$ (except $i = j = 1$). Let $\theta = \alpha + c\beta$, and consider the polynomials $g(x)$, $f(\theta - cx) \in F(\theta)[x]$.

In some extension field, $g(x)$ has roots $\beta, \beta_2, \cdots, \beta_s$; moreover, $f(\theta - c\beta_i) = f(\alpha + c(\beta - \beta_i)) \neq 0$ for $i > 1$ since $\alpha + c(\beta - \beta_i) \neq \alpha_j$. Hence $g(x)$, $f(\theta - cx)$ have just one root in common, viz $x = \beta$. Since g has no repeated roots, $\gcd(g(x), f(\theta - cx)) = x - \beta$; so $\exists\, a(x), b(x) \in F(\theta)[x]$ s.t. $a(x)g(x) + b(x)f(\theta - cx) = x - \beta$; so $\beta \in F(\theta)$, so $\alpha \in F(\theta)$. Hence $F(\alpha, \beta) = F(\theta)$. □

(work in $\bar{F}$: $F \subset E \subset \bar{F}$)

1. Integers & integral dependence

Integers are things which you can sometimes, but not always divide. This is what gave rise to different questions from those in field theory. There are no (non-trivial) real integers! In a sense, polynomials are the integral rational functions & we can do 'number theory' with them. In fact analogies between $\mathbb{Z}$ & $\mathbb{F}_q[x]$ are startling and far reaching (Deligne, Carlitz-Uchi et al) including Weil, Serre, Dwork, Katz ...).

The "Weil conjectures" are the $\mathbb{F}_q[x]$-version of the Riemann hypothesis, & have been proved by Deligne in the 1970's & 1980's with far reaching consequences. They involve a new type of cohomology theory (l-adic, or étale), which ushered in a new era of abstraction.

We shall be dealing with integers closer to home — those in some finite extension of $\mathbb{Q}$ (like the Gaussian integers). To define them we remind ourselves of integers over a ring.

All our "rings" are commutative, integral domains, with 1.

Defn. Let R be a ring, $A \subseteq R$ a subring. The element $x \in R$ is integral over A if x satisfies an equation $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, where $a_0, \ldots, a_{n-1} \in A$.

R is integral over A if all of its elements are integral over A. The next result tells us that we can add & multiply integers (i.e. that they form a ring).

7.

Proposition 1. The following are equivalent.

(i) x is integral over A.

(ii) The ring $A[x]$ is a finitely generated A-module (i.e. $\exists\ f_1, \dots, f_n \in A[x]$ s.t. $\forall f \in A[x]$ $f = \sum a_i f_i$ $(a_i \in A)$)

(iii) $\exists$ a subring B of R s.t. $A \subset B \subset R$, and $x \in B$, s.t. B is a f.g. A-module.

Pf. (i) $\Rightarrow$ (ii) Since $x^n = \sum_{i=0}^{n-1} a_i x^i$, it follows that each power x^N is an A-linear comb of $1, x, \dots, x^{n-1}$. Hence $A[x]$ is generated by these elts as A-module.

(ii) $\Rightarrow$ (iii) trivial; take $B = A[x]$.

(iii) $\Rightarrow$ (i) (the crux). Suppose B is generated as A-module by $f_1, \dots, f_r$. Then $\forall i$, we have

$$x f_i = a_{1i} f_1 + a_{2i} f_2 + \cdots + a_{ri} f_r.$$

$$\therefore (f_1 \cdots f_r)\left(A - x I_r\right) = (0, \dots, 0)$$

adj(X) = "adjugate" of X.

Multiply on the right by $\operatorname{adj}(A - xI)$, so that $(A - xI)\operatorname{adj}(A - xI) = \det(A - xI)\, I$.

It follows that $\det(A - xI) \cdot f_i = 0$ $\forall i$. Hence $\det(A - xI) = 0$.

Expanding the determinant, (i) follows. $\square$

Proposition 2. Let x, y be elements of R which are integral over A. Then $x+y$, $x-y$, & xy are integral over A.

Proof. This will follow if we show that $A[x,y] = \left\{ \sum_{i=0}^{n} a_{ij} x^i y^j \right\}$ is finitely generated over A, by Prop 1 (iii).

Now every element of $A[x,y]$ is an A-linear combination of the elts $x^i y^j$ $(i,j \in \mathbb{N})$. Hence if we exhibit a finite set of elts st. $x^i y^j$ is an A-linear comb. of them $\forall i,j$, we are done. But by integrality of x, x^i is an A-linear combin of $1, x, \cdots, x^{n-1}$ and $\cdots$ y, y^j $\cdots$ $1, y, \cdots, y^{m-1}$

It follows that $x^i y^j$ is an A-linear combin of $\{x^k y^l,\ 0 \le k \le n-1,\ 0 \le l \le m-1\}$. $\square$

Def 2. The set of elements of R which are integral over A form a ring. It is called the integral closure of A in R.

Example 0 Let $A = \mathbb{Z}$, $R = \mathbb{R}$. Then $x = \sqrt{5}$ is integral while $\sqrt[3]{\frac{5}{2}}$ is not (min poly is $t^3 - \frac{5}{2} = 0$, i.e. $2t^3 - 5 = 0$)

[Recall: a polynomial $f(x) \in \mathbb{Z}[x]$ is primitive if $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ where $\gcd(a_0, \cdots, a_n) = 1$.
Gauss' Lemma Let $f(x)$, $g(x) \in \mathbb{Z}(x)$ be primitive. Then fg is prim.
Pf. Let $f(x) = a_n x^n + \cdots + a_0$, $g(x) = b_m x^m + \cdots + b_0$. Let p be any prime. By primitivity of $f \times g$, $\exists\, i, k$ st.
$p \mid a_j$ for $j < i$ & $p \nmid a_i$, and
$p \mid b_j$ $\cdots$ $j < k$ & $p \nmid b_k$.
But then coeff of x^{i+k} in fg is $\sum_{j=0}^{i+k} a_j b_{i+k-j}$, & each term after than $a_i b_k$ is div. by p. So $\nmid p$ & $\exists$ a coeff of fg, not div by p, $\forall p$. Thus fg is primitive. $\square$]

Lemma 3. Suppose $x \in \mathbb{C}$ is integral over $\mathbb{Z}$. Then the minimal poly of x over $\mathbb{Q}$ has the form $m(t) = t^a + a_1 t^{a-1} + \cdots + a_n$, $a_i \in \mathbb{Z}$.
Pf Let $m(t)$ be the min poly of x over $\mathbb{Q}$; now x integral over $\mathbb{Z}$ $\Rightarrow$ x satisfies a poly $f(x) = X^a + a_1 X^{a-1} + \cdots + a_n = 0$, with $a_i \in \mathbb{Z}$.
We may assume

9. $g(t) = \frac{a}{b} g_1(t)$, $g_1(t) \in \mathbb{Z}[t]$, prim.
$\therefore b f(t) = a m(t) g_1(t)$.

Hence $m(t) \mid f(t)$ in $\mathbb{Q}[t]$, i.e. $\exists\ q(t) \in \mathbb{Q}[t]$ s.t. $f(t) = m(t) \cdot q(t)$.
Moreover $\exists\ a, b \in \mathbb{Z}$ s.t. $a\, m(t)$, $b\, q(t) \in \mathbb{Z}[t]$ are both primitive.
Hence $ab\, m(t) q(t) = ab\, f(t)$. But by Gauss' Lemma, $a m(t) \cdot b q(t)$ is primitive. Hence ab is a unit ($= \pm 1$). So $m(t) \in \mathbb{Z}[t]$. (i.e. $a_i \in \mathbb{Z}\ \forall i$ — a priori $a_i \in \mathbb{Q}$). Let $i \to \infty$. □

Cor 3: Suppose $x \in \mathbb{Q}$ is integral over $\mathbb{Z}$. Then $x \in \mathbb{Z}$.
Pf. If x is integral, x has min poly $x - \frac{p}{q} = 0$ s.t. $\frac{p}{q} \in \mathbb{Z}$ by Lemma 3. □

Defn. An integral domain is integrally closed if it is its own integral closure in its quotient field.
example. $\mathbb{Z}$ is integrally closed.

To complete this introduction to integers we investigate what happens if one takes repeated integral closures.

Proposition 4. Let $A \subset B \subset C$ be integral domains. If C is integral over B and B is int over A, then C is integral over A.
Pf. Any $x \in C$ satisfies an equation $x^n + b_1 x^{n-1} + \cdots + b_n = 0$.
Let $B' = A[b_1, \ldots, b_n]$; then x is integral over B'.
But the b_i are integral over A so by the proof of Prop 1 (ii), $A[b_1, \ldots, b_n, x]$ is finitely generated over A. Hence, by Prop 1 (i), x is integral over A. □.

Cor 4: If $\bar{A}$ = integral closure of A in R, then $\bar{\bar{A}} = \bar{A}$.

Lemma 5: Let $A \subset R$ be integral domains.
(i) The integral closure $\bar{A}$ of A in R is int. closed in R.
(ii)

Proposition Lemma 5: (i) The integral closure of an int dom. A (in its quotient field) is int closed.
(ii) Any PID is int. closed.

Proof (i) Let K = quot. field of A, $\bar{A}$ = integral closure of A in K. Then quot. field of $\bar{A}$ is also K & $\bar{\bar{A}} = \bar{A}$ so $\bar{A}$ is int. closed.
(ii) Let A be a PID, K its quot. field. Then Theorem since proposition we have Gauss' Lemma for $A[t]$, the same proof as in Lemma 3 shows that a/b integral over $A \Rightarrow a/b \in A$. □

[Ex: give a direct proof: $(a/b)^n = \sum_{i=0}^{n-1} a_i (a/b)^i$; so $a^n = b\left(\text{---}\right)$, hence any prime divisor of b divides a. $\Rightarrow \frac{a}{b} \in A$.]

over

11.

§2 Algebraic integers.

(2.1) Alg Number Fields.

A finite (hence algebraic) extension field of $\mathbb{Q}$ will be called an algebraic number field. By the Thm of the Primitive elt any alg number fld F is of the form $F = \mathbb{Q}(\alpha)$, with α algebraic over $\mathbb{Q}$.

Where convenient, we shall think of F as lying inside a fixed copy of $\mathbb{C}$.

Defn. An algebraic integer is an element of an algebraic number field F which is integral over $\mathbb{Z}$.

By §1, the set of algebraic integers in F forms a ring.

Remark. If $z \in F$ is an algebraic integer, then any algebraic conjugate of z (i.e. elt of $\mathbb{C}$ with the same min poly) is also an algebraic integer.

For if $m(z) = 0$ is an eqn of integral dependence, then $\sigma(m(z)) = m(z^\sigma) = 0$ for any $\sigma \in Gal(\tilde{F}/\mathbb{Q})$ $\tilde{F}$ = normal algebraic closure of F.

Bad example $z^3 = 2$ has 3 roots: z_0 (real) $= \sqrt[3]{2}$, $z_0\omega$, $z_0\omega^2$, $\omega = \exp\left(\frac{2\pi i}{3}\right)$.
Let $F = \mathbb{Q}(z_0) \subseteq \mathbb{R}$. Then the conjugates of z_0 are not in F. (i.e. F may not be a Galois extension).

Lemma 1. If F is an algebraic number field, then F is the quotient fld of its ring of integers.

Pf. Let $\theta \in F$. Then θ is a root of $f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0$, with $a_i \in \mathbb{Q}$ (since θ is algebraic). Write $a_i = \frac{b_i}{b}$ (common denominator), with $b_i, b \in \mathbb{Z}$.

Then $f(x) = x^b + \frac{b_{b-1}}{b} x^{b-1} + \cdots + \frac{b_0}{b}$, & multiplying by b^b: $f(x) \cdot b^b = (bx)^b + b_{b-1}(bx)^{b-1} + \cdots + b_0'$, where $b_i' \in \mathbb{Z}$.

Hence $b\theta$ is an integer in F & $\theta = b\theta/b$. □

(We've shown: any elt of F is the quotient of an alg integer by a rational integer).

(2.2) Quadratic fields.

Example. Integers in quadratic number fields.

F is called quadratic if $\dim_{\mathbb{Q}}(F/\mathbb{Q}) = \dim_{\mathbb{Q}}(F) = 2$.

In this case $F = \mathbb{Q}(\alpha)$ with α satisfying an equation

$x^2 + bx + c = 0$, $b, c \in \mathbb{Q}$.

$\therefore 2\alpha = -b \pm \sqrt{b^2 - 4c}$

Since $\mathbb{Q}(\alpha) = \mathbb{Q}(2\alpha + b)$, we see that $F = \mathbb{Q}(\sqrt{b^2 - 4c})$.

Hence:

Lemma 2. Every quadratic field is of the form $F = \mathbb{Q}(\sqrt{d})$, where d is a square free integer

If. We've seen that $F = \mathbb{Q}\left(\sqrt{\frac{p}{q}}\right) = \mathbb{Q}\left(q\sqrt{\frac{p}{q}}\right)$.

$= \mathbb{Q}(\sqrt{pq})$.

$\Rightarrow F = \mathbb{Q}(\sqrt{d})$ where d is an integer, and evidently may be taken to be square free. (since p, q have no common factors) □.

It follows that F is a normal extension of $\mathbb{Q}$, because the only conjugate of $a + b\sqrt{d}$ $(a, b \in \mathbb{Q})$ is $a - b\sqrt{d}$. Write $\mathrm{Gal}(F/\mathbb{Q}) = \{1, \sigma\}$, where $(\sqrt{d})^\sigma = -\sqrt{d}$.

Suppose $x = a + b\sqrt{d}$ is an integer. Then $x x^\sigma = (a + b\sqrt{d})(a - b\sqrt{d})$

$= a^2 - b^2$

Def: Let A = ring of integers in $\mathbb{Q}(\sqrt{d})$;

Then A = integral closure of $\mathbb{Z}$ in F.

If $x \in A$ then $\sigma(x) \in A$, because x, $\sigma(x)$ have the same min polynomial.
$\therefore$ $\sigma(x) = a^2 - db^2 \in A \cap \mathbb{Q}$. $= \mathbb{Z}$. Hence, $x = a + b\sqrt{d}$ an integer $\Rightarrow$ $a^2 - db^2 \in \mathbb{Z}$, and $2a \in \mathbb{Z}$.
Conversely, if $a^2 - db^2 \in \mathbb{Z}$ then $x^2 - 2ax + (a^2 - db^2)$ is an equation of integral dependence over $\mathbb{Z}$.
Conclusion $a + b\sqrt{d}$ is an integer $\Leftrightarrow$ $\begin{cases} a^2 - db^2 \in \mathbb{Z}. \\ \text{and } 2a \in \mathbb{Z}. \end{cases}$

Proposition 3. Let $F = \mathbb{Q}(\sqrt{d})$ where d is a square free integer. Then
(i) If $d \equiv 1 \pmod 4$, A (the ring of integers in F) $= \left\{ \frac{1}{2}(u + v\sqrt{d}) \mid \begin{matrix} u, v \in \mathbb{Z} \\ u \equiv v \pmod 2 \end{matrix} \right\}$

(ii) If $d \equiv 2$ or $3 \pmod 4$ then $A = \{ u + v\sqrt{d} \mid u, v \in \mathbb{Z} \}$

Proof: We've seen that $a + b\sqrt{d}$ is an integer $\Leftrightarrow a^2 - db^2 \in \mathbb{Z}$ and $2a \in \mathbb{Z}$.
But $a^2 - db^2 \in \mathbb{Z} \Rightarrow 4a^2 - 4db^2 \in \mathbb{Z} \Rightarrow 4db^2 \in \mathbb{Z}$
$\Rightarrow d \cdot (2b)^2 \in \mathbb{Z}$. But d is square free, so if $2b \notin \mathbb{Z}$,
$d = \frac{m \cdot q^2}{q^2}$, would be a contradiction.
So $2b \in \mathbb{Z}$. Write $a = \frac{u}{2}$, $b = \frac{v}{2}$ where $u, v \in \mathbb{Z}$.
Then $u^2 - dv^2 \in 4\mathbb{Z}$. $(= (2a)^2 - d \cdot (2b)^2)$
Thus: either u, v are both even or v is odd (v even $\Rightarrow u$ even
in which case $v^2 \equiv 1 \pmod 4$ & $u^2 \equiv d \pmod 4$, so u is odd &
$d \equiv 1 \pmod 4$. This completes the proof. □.

L3↓.

Notation If $d > 0$ F is real quadratic
$d < 0$ - - - imaginary quadratic

Examples: (i) $\frac{1+\sqrt{5}}{2}$ is an integer.
(ii) If $d = -1 \equiv 3 \pmod 4$, the integers in $\mathbb{Q}(\sqrt{-1})$ are $\{n + mi \mid m, n \in \mathbb{Z}\}$. These are the "Gaussian integers".

§3. Norms, traces and discriminants.

Suppose B is an integral domain, & $A \subset B$ is a subring such that B is a free A-module of finite rank. Then B has a finite A-basis $b_1, \dots, b_n$, & any element of B has a unique expression

$$b = \sum_{i=1}^{n} a_i b_i, \qquad a_i \in A.$$

Example. (Canonical example in this course).
Let A be a field, B an algebraic extension of A of degree n. Then "A-module" is just a vector space over A, and "free of rank n" means $\dim_A B = n$.

In this situation, if $x \in B$ then x defines an A-module endomorphism $m_x : b \longmapsto xb$

Definition. We define the functions $Tr_{B/A}$ and $N_{B/A} : B \to A$ by
$$Tr(x) = tr(m_x).$$
$$N(x) = \det(m_x).$$

Explicitly, if $xb_i = \sum_{j=1}^{n} a_{ij} b_j$, then $Tr_{B/A}(x) = \sum_{i=1}^{n} a_{ii}$

and $N_{B/A}(x) = \det(a_{ij})$.

Note that the characteristic poly of x (i.e. of m_x) is $\det(tI - a_{ij})$. This is monic in $A[t]$ & hence B is integral over A (by Prop 1). (as we already know, as B is f.g. mod A)

Since $(x+y)b = xb + yb$, $m_{x+y} = m_x + m_y$
& Sim, $m_{xy} = m_x m_y$, and $a \cdot m_x = m_{ax}$.

$\therefore$ Tr and N satisfy:

$$\begin{cases} \mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y). \\ \mathrm{Tr}(ax) = a\,\mathrm{Tr}(x). \\ \mathrm{Tr}(a) = na \quad (n = [B:A]). \quad (a \in A). \quad n = \mathrm{rk}_A(B). \\ N(xy) = N(x)N(y). \\ N(a) = a^n \\ N(ax) = a^n N(x). \\ N(1) = 1. \end{cases} \quad (*)$$

L, K are number fields and

Lemma 1. Suppose $\mathbb{C} \supset L \supset K$ where $[L:K] = n$. Let $x \in L$ and if $m_x(t)$ is the min poly of x over K let $x = x_1, x_2, \dots, x_r \in \mathbb{C}$ be the roots of $m(t)$ in $\mathbb{C}$. If $s = [L : K(x)]$ we have $\mathrm{Tr}_{L/K}(x) = s(x_1 + \cdots + x_r)$

$$\begin{array}{ccc} L & \supseteq & K(x) \supseteq K \\ & s & \quad r \end{array}$$

& $N_{L/K}(x) = (x_1 \cdots x_r)^s$

Moreover (it follows that) we have $C_{m_x}(t) = \left[(t-x_1)\cdots(t-x_r)\right]^s$

Pf. Let $C_{m_x}(t)$ be the char poly of $m_x : L \to L$. Then the roots of $C_{m_x}(t)$ are all roots of $m(t)$, because we may write $m_x \sim \begin{pmatrix} y_1 & * & \\ & y_2 & \\ 0 & & \ddots \\ & & & y_n \end{pmatrix}$ & hence $m(m_x) = 0 \Rightarrow m(y_i) = 0 \ \forall i$

suffices to take $Gal(\bar{L}/K)$.

Moreover by Cayley–Hamilton, $m(t) \mid C_x(t)$. Since $C_x(t)$ is invt under $Gal(\bar{\mathbb{Q}}/K)$, each root of $m(t)$ occurs in $C_x(t)$ with the same multiplicity. Hence $C_x(t) = c \cdot m(t)^s$, $c \in K^\times$. The result is now clear. □.

Cor 1' A K-isom : $L \to \mathbb{C}$ is an embedding $\sigma: L \to \mathbb{C}$ such that $\sigma(kl) = k\,\sigma(l)$ $(k \in K,\ l \in L)$.
Let $\sigma_1, \dots, \sigma_n$ be the distinct K-isoms of L into $\mathbb{C}$.
Then $Tr(x) = \sum \sigma_i(x)$, and $N(x) = (-1)^n \prod_i \sigma_i(x)$,
and $C_x(t) = \prod(t - \sigma_i(x))$. (note: $n = [L:K]$).

Pf: Let $x \in L$ and let $m(t)$ be the min poly of x over K. By the theorem of the prim element, $L = K(y)$ & if $y_1, \dots, y_n$ are the conjugates of y over K, then $\sigma_i : y \mapsto y_i$ defines the embedding σ_i.
~~Now $x = f(y)$: hence the conjugates of x over K are the $f(y_i)$ (repeated n/r times).~~
Now $g(t) := \prod(t - \sigma_i(x)) \in K[t]$ and $g(x) = 0 \Rightarrow m(t) \mid g(t)$.
Hence $m(t) = \prod(t - \sigma_i(x))$, & $C_x(t) = g(t)$. □.
distinct factors.

Proposition 2. Let A be an integral domain, $A \subset K \subset L \subset \mathbb{C}$, K its quotient field, L a finite (degree n) extension of K. Let $x \in L$ be integral over A. Then the coeffts of the char poly $C_x(t)$ & min poly $m_x(t)$ for L/K are integral over A.
Pf. With notation as above, the conjugates x_i of x satisfy the same equation of integral dependence as x; hence they are integral over A. But $C_x(t) = \prod(t-x_1)^s \cdots (t-x_r)^s$, & so $C_x(t)$ has coeffts which are integral over A. □

NB Conjugate of y over K ≡ root of the min poly $m_y(t)$ over K.

Cor 2' We have, with the hypotheses of Prop 2,

$\left.\begin{matrix} Tr_{L/K}(x) \\ N_{L/K}(x) \end{matrix}\right\}$ are integral over A.

Cor 2'' If in Prop 2 A is integrally closed (say in K), then the coeffs of $C_x(t)$, $\pm m_x(t)$ are in A, and $N_{L/K}(x)$, $Tr_{L/K}(x)$ are in A.

Pf. Any elt of K which is integral over A is in A. □

Discriminants

Let $A \subset B$ be integral domains, with B a free A-module of rank n. Let $(x_1, \dots, x_n) \in B^n$ (an ordered n-tuple). Define the discriminant $\Delta(x_1, \dots, x_n)$ by

$$\Delta(x_1, \dots, x_n) = \det\left(Tr_{B/A}(x_i x_j) \right)_{i,j}.$$

Δ changes under A-linear transformations as follows:

Lemma 3 Let $y_i = \sum_{j=1}^{n} a_{ij} x_j \quad (i = 1, \dots, n)$.

Then $\Delta(y_1, \dots, y_n) = \left[\det(a_{ij})\right]^2 \Delta(x_1, \dots, x_n)$.

Pf. We have $Tr(y_i y_j) = Tr\left(\sum_{k=1}^{n} a_{ik} x_k \sum_{\ell=1}^{n} a_{j\ell} x_\ell \right)$

$$= Tr\left(\left(\sum_{k=1}^{n} \sum_{\ell=1}^{n} a_{ik} a_{j\ell} \right) x_k x_\ell \right).$$

$\therefore$ in matrix terms $\left(Tr(y_i y_j)\right) = \left(A \left(Tr(x_k x_\ell)\right) A^t\right)_{ij}$

$\therefore \det\left(Tr(y_i y_j)\right) = (\det A)^2 \det\left(Tr(x_i x_j)\right)$. □

Suppose that $b_1, \dots, b_n$ and $b_1', \dots, b_n'$ are two bases of B over A.

Then $b_i' = \sum_{j=1}^{n} a_{ij} b_j$, where (a_{ij}) is invertible (over A).

$\therefore$ $\det(a_{ij})$ is a unit in A.

Hence:

Cor 3' If $(x_1, \dots, x_n)$ and $(y_1, \dots, y_n)$ are bases of B/A then $D(x_1, \dots, x_n)$ and $D(y_1, \dots, y_n)$ are associates in A. In particular, they generate the same principal ideal of A.

Defn. The discriminant of B over A is the principal ideal of A generated by $D(x_1, \dots, x_n)$ for any basis $(x_1, \dots, x_n)$ of B. Denote this discriminant by $\Delta_{B/A}$.

Lemma 4. Suppose $\Delta_{B/A} \neq 0$. Then an element $(x_1, \dots, x_n) \in B^n$ is a basis of B over $A \iff D(x_1, \dots, x_n)$ generates $\Delta_{B/A}$

Pf: If $x_1, \dots, x_n$ is a basis the second statement is just the definition of $\Delta_{B/A}$.

Conversely if $D(x_1, \dots, x_n)$ generates $\Delta_{B/A}$, then for some basis $b_1, \dots, b_n$ we have $x_i = \sum a_{ij} b_j$ and $D(x_1, \dots, x_n) = (\det A)^2 D(b_1, \dots, b_n)$. It follows that $(\det A)^2$ is a unit in A, so $\det A$ is a unit, whence A is invertible. □

Dedekind's lemma. Let G be any group and $\sigma_1, \dots, \sigma_n$ distinct group homomorphisms $\sigma_i : G \to \mathbb{C}^\times$. Then the σ_i are linearly indept over $\mathbb{C}$ — i.e. $\sum \lambda_i \sigma_i = 0$ $(\lambda_i \in \mathbb{C}) \Rightarrow \lambda_i = 0 \ \forall i$.

Proof. Suppose $\lambda_1 \sigma_1 + \cdots + \lambda_q \sigma_q = 0$ with q minimum, and $\lambda_1, \lambda_2 \neq 0$ (notation). Then for $h, g \in G$ all $\lambda_i \neq 0$.

$\lambda_1 \sigma_1(h) \sigma_1(g) + \cdots + \lambda_q \sigma_q(h) \sigma_q(g) = 0$. and

subtracting $\lambda_1 \sigma_1(g) \sigma_1(h) + \lambda_2 \sigma_2(g) \sigma_2(h) + \cdots + \lambda_q \sigma_q(g) \sigma_q(h) = 0$.

Subtracting, we obtain $\forall g, h \in G$:

$$0 = \lambda_1 \sigma_1(g)\big(\sigma_1(h) - \sigma_1(h)\big) + \lambda_2 \sigma_2(g)\big(\sigma_2(h) - \sigma_1(h)\big) + \cdots + \lambda_q\big(\sigma_q(h) - \sigma_1(h)\big)$$

By minimality of q, we conclude that $\forall h$, $\sigma_1(h) = \sigma_2(h)$, i.e. $\sigma_1 = \sigma_2$ ✗ □

This will enable us to show that in many important cases, $\Delta_{B/A}$ is the discriminant of a non-degenerate bilinear form.

Proposition 5: Suppose $K \subset L \subset \mathbb{C}$, and $[L:K] = n$.
Let $\sigma_1, \ldots, \sigma_n$ be the distinct K-isomorphisms of $L \hookrightarrow \mathbb{C}$.
[They correspond to $\theta \mapsto \theta_i$, where $L = K(\theta)$, and $\theta_1, \ldots, \theta_n$ are the roots of $m_\theta(t)$]
If $(x_1, \ldots, x_n)$ is a K-basis of L (could be powers of θ), then $D(x_1, \ldots, x_n) \neq 0$ & in fact $D(x_1, \ldots, x_n) = \det\big(\sigma_i(x_j)\big)^2$.

Proof. By Cor 1', $\mathrm{Tr}(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j)$

Hence $\det\big(\mathrm{Tr}(x_i x_j)\big)_{ij} = \det\Big(\sum_k \sigma_k(x_i)\sigma_k(x_j)\Big)_{ij}$

$= \det(\Sigma \Sigma^t)$, (where $\Sigma_{ik} = \sigma_k(x_i)$)

$= (\det \Sigma)^2$

$= \det\big(\sigma_i(x_j)\big)^2$.

Now by Dedekind's lemma the $\sigma_i : L \to \mathbb{C}$ are linearly indep over $\mathbb{C}$, so that the rows of Σ are linearly dependent. Hence $\det \Sigma \neq 0$. □.

15-8-17.

is given a K-basis $x_1, \dots, x_n$ of L,

Cor 5' With notation as in Prop 5, $\exists$ a basis $y_1, \dots, y_n$ of L over K such that $\mathrm{Tr}(x_i y_j) = \delta_{ij}$.

Proof. Let $T = (t_{ij})$ be the matrix with (i,j) entry $t_{ij} = \mathrm{Tr}(x_i x_j)$. Prop 5 says that T is non-singular. Hence the map (bilinear) $\tau(x,y) \mapsto \mathrm{Tr}(xy)$ is non-degenerate. In fact if $x = \sum_{i=1}^n a_i x_i$ and $y = \sum_{i=1}^n b_i x_i$ $(a_i, b_j \in K)$ we have $\tau(x,y) = \underline{a}^t T \underline{b}$, where $\underline{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ etc.

Hence the basis $x_1, \dots, x_n$ of L has a unique dual basis $y_1, \dots, y_n$ wrt τ, and $\tau(x_i, y_j) = \delta_{ij} = \mathrm{Tr}(x_i y_j)$. ☐

The map $\tau_x : y \mapsto \tau(x,y)$ is K-linear: $L \to K$, and $\mathcal{L}$ is the space of all such $\mathcal{L} = \{\tau_y\}$.

[More elementary explanation: the maps $y \mapsto \tau(x_i, y)$ form a basis of L^* (dual K-vector space). So there are unique y_i s.t. $y \mapsto \tau(y_i, y)$ sends x_j to δ_{ij}.]

Applying this to our integral setup, we obtain

Theorem 6. Let A be an integrally closed integral domain with quotient field K. Suppose L is a finite, degree n extension of K s.t. $A \subset K \subset L \subset \mathbb{C}$. If A' is the integral closure of A in L, then A' is a finitely generated A-module of a free A-module of rank n.

Proof. Let $x_1, \dots, x_n$ be a basis of L over K. Since the x_i are algebraic over K, the same argument as in Lemma 1 of §2 shows that $\forall i$, $\exists a_i \in A$ such that $a_i x_i \in A'$.

[Argument: x alg $\Rightarrow \exists$ poly $t^m + b_1 t^{m-1} + \cdots + b_m = f(t)$, s.t. $f(x) = 0$, $b_i = \frac{a_i}{c_i}$ $(a_i, c_i \in A)$. Let $c = \prod c_i$. Then $c^m f(t) = (ct)^m + c b_1 (ct)^{m-1} + \cdots + c^m b_m$,

So $c^n f(t) = g(ct)$, where $g(y) \in A[y]$, and $g(cx) = 0$.
$\therefore$ ~~cx~~ cx is integral over A & hence is in A'.]

Hence, after replacing the x_i by the $a_i x_i$, we may assume that the $x_i \in A'$ (i.e. are integral over A).
Now let $y_1, \dots, y_n \in L$ be such that $\mathrm{Tr}(x_i y_j) = \delta_{ij}$ (cf. Cor 5' above). We show that every element of A' may be written as an A-linear combination of the y_i.
Take $x \in A'$; since the y_i are a basis of L/K, $\exists\, b_i \in K$ such that $x = \sum_{i=1}^{n} b_i y_i$. But then

$\mathrm{Tr}(x_i x) = b_i \in A$ by Cor 2'. Hence
$A \subset \bigoplus_{i=1}^{n} A y_i$, free A-module with basis $\{y_i\}$. □

(*) (NB) **Cor 6'** If A in Thm 6 is a PID, then A' is a free A-module of rank n.

Pf: $\sum A y_i$ is a free module over a PID, whence A' is free on a basis of rank $r \le n$. But A' contains a basis of L/K. So rank $A' = n$. □

Applying these conclusions to number fields:

(*) (NB) **Cor 6''** Suppose F is an algebraic number field with ring of integers A. Then A is a free abelian group of rank $n = [F : \mathbb{Q}]$.

Definition. $(a_1, \dots, a_n)$ is an integral basis of A if $a_1, \dots, a_n$ generate A as a f.a.g.

(Quadratic Fields)

Example. Let $F = \mathbb{Q}(\sqrt{d})$ where d is square free.

If $d \equiv 2$ or $3 \pmod 4$, an integral basis is $\{1, \sqrt{d}\}$.

If $d \equiv 1 \pmod 4$, ——— $\left\{\frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}\right\}$.

[This is immediate from §2 Prop 3 (p13)]

Thurs 17-8-17

Defn. The discriminant of an algebraic number field F is the discriminant of any integral basis, of its ring of integers.

Remark. If $\theta_1, \dots, \theta_n$ & another integral basis of F, then $D(\theta_1, \dots, \theta_n)$ is independent of the basis since any unit in $\mathbb{Z}$ which is a square is $+1$. So not only is $\Delta_{F/\mathbb{Q}}$ (the principal ideal) well defined, but $D(\text{integral basis})$ is well defined. (Discrim $\in \mathbb{Z}$)!!

Example (Quadratic fields).

Let $F = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ is square free.

① If $d \equiv 2$ or $3 \pmod 4$ then an integral basis $\{1, \sqrt{d}\}$ &

$$D(1, \sqrt{d}) = \begin{vmatrix} \mathrm{tr}(1) & \mathrm{tr}(\sqrt{d}) \\ \mathrm{tr}(\sqrt{d}) & \mathrm{tr}(d) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d.$$

② If $d \equiv 1 \pmod 4$ then an integral basis $\left\{\frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}\right\}$

Exercise ($d \equiv 1$). (i) Show $\left(\frac{1+\sqrt{d}}{2}\right)^2 = a\left(\frac{1+\sqrt{d}}{2}\right) + b\left(\frac{1-\sqrt{d}}{2}\right)$ where

$a = \frac{d+3}{4}$, $b = \frac{d-1}{4}$.

(ii) Deduce that $\mathrm{tr}\left(\frac{1+\sqrt{d}}{2}\right) = 1$

(iii) Similarly, deduce that $\mathrm{tr}\left(\frac{1-\sqrt{d}}{2}\right) = 1$.

(iv) Deduce then or otherwise, show that

$$D\left(\frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}\right) = \begin{vmatrix} \frac{d+1}{2} & \frac{1-d}{2} \\ \frac{1-d}{2} & \frac{d+1}{2} \end{vmatrix} = d.$$

23 Computing discriminants.

Wlog assume x is integral over $\mathbb{Z}$ (replace by nx).

Lemma 7 Let $L = K(x) \subseteq \mathbb{C}$ be a finite (Kyja) extension, let $m(t)$ be the minimal polynomial of x over K. Then the discriminant of the basis $(1, x, \cdots, x^{n-1})$ is given by

$$D(1, x, x^2, \cdots, x^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{L/K}(m'(x)) = \prod_{i=1}^{n} m'(x_i) \cdot (-1)^{\frac{1}{2}n(n-1)},$$

where $m'(t) = \frac{dm}{dt}$.

Pf. Let $x_1, \cdots, x_n$ be the roots of $m(t)$ in $\mathbb{C}$. Then by Prop 5

$$D(1, x, \cdots, x^{n-1}) = \det\left(\sigma_i(x^j)\right)^2$$

$$= \det\left(x_i^j\right)^2$$

$$= \begin{vmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ \vdots & & & \\ 1 & x_n & \cdots & x_n^{n-1} \end{vmatrix}^2$$

$$= (-1)^{\frac{1}{2}n(n-1)} \prod_{j \neq i} (x_i - x_j) \quad (\text{all } i \neq j).$$

$$= (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} \left(\prod_{j \neq i} (x_i - x_j) \right)$$

$$= \prod_{i=1}^{n} m'(x_i) \cdot (-1)^{\frac{1}{2}n(n-1)} (-1)^{\frac{1}{2}n(n-1)} \quad * \quad \checkmark$$

$$= N_{L/K}(m'(x)). \quad \square$$

* Use $m(t) = \prod_{i=1}^{n} (t - x_i)$, so $m'(t) = \sum_{i=1}^{n} \left(\prod_{j \neq i} (t - x_j) \right)$.

Example. Suppose $L = K(x)$, where $m(t) = t^n + at + b$ (assumed to be irreducible). Let the roots of $m(t)$ in $\mathbb{C}$ be $x = x_1, x_2, \cdots, x_n$. We have $m'(t) = nt^{n-1} + a$.

$$\therefore N(m'(x)) = \pm m'(x_1)\, m'(x_2) \cdots m'(x_n).$$

$$= \prod_{i=1}^{n} (n x_i^{n-1} + a)$$

$$= \prod_{i=1}^{n} x_i^{-1} \left(n x_i^n + a x_i\right)$$

$$= b^{-1}(-1)^n \prod_{i=1}^{n} \left(n(-a x_i - b) + a x_i\right) \qquad \text{since } \prod x_i = (-1)^n b$$

$$= (-1)^n b^{-1} \prod_{i=1}^{n} a(1-n)\left(x_i - \frac{nb}{a(1-n)}\right)$$

Since $\prod (t - x_i) = t^n + at + b$, we have:

$$N(m'(x)) = (-1)^n b^{-1} a^n (1-n)^n \left(\left(\frac{nb}{a(1-n)}\right)^n + a\frac{nb}{a(1-n)} + b\right).$$

$$= n^n b^{n-1} + \frac{n}{1-n} \cdot a^n (1-n)^n + a^n (1-n)^n$$

$$= n^n b^{n-1} + a^n (1-n)^{n-1} (1 - n + n)$$

$$= n^n b^{n-1} + a^n (1-n)^{n-1}.$$

Examples $n = 2$: $N = 4b - a^2$.

$n = 3$: $N = 27b^2 + 4a^3$.

$n = 4$: $N = 256 b^3 - 27 a^4$.

These are well-known discriminants of polynomials which occur in solutions by radicals.

We'll see later how Δ influences the structure of the ring of integers.

§4 Cyclotomic fields – I

A cyclotomic field is one which is generated over $\mathbb{Q}$ by roots of unity. Let p be an odd prime & $z \in \mathbb{C}$ a primitive p^{th} root of unity. Then z is a root of $t^p - 1$ & we have

Lemma 1. If z is a primitive p^{th} root of unity then z has minimal polynomial $m(t) = \dfrac{t^p - 1}{t - 1} = 1 + t + \cdots + t^{p-1}$.

Pf: Since $z^p = 1$ and $z \neq 1$, $m(z) = 0$. It therefore suffices to show that $m(t)$ is irreducible in $\mathbb{Q}[t]$. This will follow from:

Eisenstein's criterion Let A be a PID, $p \in A$ prime. If $f(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in A[t]$ and $p \mid a_i$ $\forall i$ but $p^2 \nmid a_n$ (constant term) then $f(t)$ is irreducible over the quot fld of A. (irred/A $\equiv$ irred/K = quot fld of A).

Pf of Eisenstein: If $f(t) = g(t)h(t)$ then by Gauss' lemma, we may take $g(t), h(t) \in A[t]$. Now take the coeffs of f, g, h mod p: $\bar{f} = \bar{g}\bar{h} = t^n$. But $A/\langle p \rangle$ is an integral domain (p prime) & so $\bar{g}$ and $\bar{h}$ must be monomial (otherwise get 2 non-zero powers). $\therefore \bar{g} = t^k$ $\bar{h} = t^{n-k}$. But then $p \mid$ all coeffs of $\bar{g}, \bar{h}$ except the highest; so $p^2 \mid a_n = g_0 h_{n-k}$ ⋇ □

Pf of lemma 1. Write $t = u + 1$; then $m(t) = m_1(u) = \dfrac{(u+1)^p - 1}{u}$

$= \displaystyle\sum_{j=0}^{p-1} \binom{p}{j} u^{j-1}$, & $m_1(u)$ is irred by Eisenstein. □

Cor 1' $m(t)$ is irred.

Cor 1'' $\mathbb{Q}(z)$ has degree $p-1$ over $\mathbb{Q}$. Moreover $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q}) \cong C_{p-1}$

Cor 1''' $\mathbb{Q}(z)$ has basis $1, z, z^2, \ldots, z^{p-2}$ over $\mathbb{Q}$. (integral basis).

$m(t)$ is the "p^{th} cyclotomic polynomial".

What are the integers in $\mathbb{Q}(z)$?

Thm 2. The integers in $\mathbb{Q}(z)$ are $\{\sum_{i=0}^{p-2} a_i z^i \mid a_i \in \mathbb{Z}\}$.

That is, $\{1, z, \cdots, z^{p-2}\}$ is an integral basis of the subring of integers in $\mathbb{Q}(z)$.

Pf Suppose $x \in A$, $x = a_0 + a_1 z + \cdots + a_{p-2} z^{p-2}$, $a_i \in \mathbb{Q}$.

RTP: $a_i \in \mathbb{Z}$.

Now $\mathrm{Tr}(x) = a_0 \mathrm{Tr}(1) + a_1 \mathrm{Tr}(z) + \cdots + a_{p-2} \mathrm{Tr}(z^{p-2})$

$= a_0(p-1) - a_1 - a_2 - \cdots - a_{p-2}$

(since for $i = 1, \cdots, p-1$, z^i is a prim. p^{th} root of 1, & has min poly $m(t) = 1 + t + \cdots + t^{p-1}$; so sum of conjs $= -1$).

$= p a_0 - \sum_{i=0}^{p-2} a_i \in \mathbb{Z}$.

Since $z \in A$, $zx = a_0 z + \cdots + a_{p-2} z^{p-1} \in A$.

$\therefore \mathrm{Tr}(zx) = -\sum_{i=0}^{p-2} a_i \in \mathbb{Z}$ by the above.

$\therefore p a_0 \in \mathbb{Z}$ $(= \mathrm{Tr}(x(1-z)))$. 22-8

It therefore suffices to show: [Since $\mathrm{Tr}(x(1-z)) = p a_0$]

(*) $\mathrm{Tr}(x(1-z)) \in p\mathbb{Z}$. [For then, $a_0 \in \mathbb{Z}$, so $a_1 z + \cdots + a_{p-2} z^{p-2} \in A$, so $z^{p-1}(-) \in A$; so $a_i \in \mathbb{Z}$ $\forall i$.]

Proof of (*). The conjugates of $y(1-z)$ are of the form $y'(1-z^j)$ $(y \in A)$ — apply elts of $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q})$ $\sigma_j : z \mapsto z^j$. $\in A(1-z)$. Hence $\mathrm{Tr}(y(1-z)) \in A(1-z) \cap \mathbb{Z}$.

But $\prod_{i=1}^{p-1} (t - z^i) = m(t) = 1 + t + t^2 + \cdots + t^{p-1}$

$\therefore \prod_{i=1}^{p-1} (1 - z^i) = m(1) = p \quad (i = 1, \cdots, p-1)$.

Now $p\mathbb{Z}$ is a max'l ideal in $\mathbb{Z}$. So $A(1-z) \supseteq \prod(1-z^i) = p$, so $A(1-z) \cap \mathbb{Z} \supseteq p\mathbb{Z}$. If $A(1-z) \cap \mathbb{Z} = \mathbb{Z}$, then $1-z$ would be invertible in A. But the conjugates of $1-z$ are $1-z^i$, $i = 1, 2, \cdots, p-1$, Hence each of these factors is invertible in A, and so $\prod_{i=1}^{p-1}(1-z^i) = p$ is invertible in A.

That is, $\exists\ \alpha \in A$ s.t. $\alpha p = 1$. But $\alpha = \frac{1}{p}$ & so we conclude that $\frac{1}{p}$ is integral over $\mathbb{Z}$ & hence $\frac{1}{p} \in \mathbb{Z}$ ⚡.

It follows that $A(1-z) = p\mathbb{Z}$. Hence
$\mathrm{Tr}(x(1-z)) = a_0 p \in p\mathbb{Z}$, so that $a_0 \in \mathbb{Z}$.
But then one derives easily that $a_i \in \mathbb{Z}\ \forall i$. □

Cor 21 $\mathbb{Q}(z)$ has integral basis $\{1, z, \cdots, z^{p-2}\}$.

Exercise. Show that $D(1, z, \cdots, z^{p-2}) = p^{p-2} \cdot (-1)^{\frac{p-1}{2}}$ (p odd)

Solution. In this case we have $m(t) = 1 + t + \cdots + t^{p-1} = \dfrac{t^p - 1}{t-1}$

& the min poly of $z, \cdots, z^{p-2}$. The distinct embeddings $\mathbb{Q}(z) \hookrightarrow \mathbb{C}$ are given by $\sigma_i\ (z \mapsto z^i)$ $(i = 1, 2, \cdots, p-1)$.

$$\therefore D(1, z, \cdots, z^{p-2}) = \det\left(z^{ij}\right)^2_{\substack{i=1,\cdots,p-1 \\ j=0,\cdots,p-2}}$$

$$= \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ z & z^2 & & z^{p-1} \\ z^2 & & & \\ \vdots & & & \\ z^{p-2} & & & \end{pmatrix}^2$$

$$= \left(\prod_{1 \le i < j \le p-1} (z^i - z^j) \right)^2$$

$$= \left(z^{1+2+\cdots+p-2} \left(\prod_{k=1}^{p-2} (1 - z^k) \right) \right)^2$$

Note: $z \cdot z^2 \cdots z^{p-1} =$ product of roots of $1 + t + t^2 + \cdots + t^{p-1} = 0$.
$= (-1)^{p-1}$

$\therefore A^{1+2+\cdots+p-2} = (-1)^{p-1} z^{1-p} = (-1)^{p-1} z$.

& norm $= z^{2(1-p)} = z^2$

$$= (-1)^{\frac{1}{2}p(p-1)} \prod_{i=1}^{p-1} \prod_{j \neq i} (z^i - z^j)$$

Now $m(t) = 1 + t + t^2 + \cdots + t^{p-1}$ has roots $\{z^i \mid i = 1, \cdots, p-1\}$;

so $= \prod_{i=1}^{p-1} (t - z^i)$. Hence

$m'(t) = 1 + 2t + 3t^2 + \cdots + (p-1)t^{p-2}$ satisfies

(b) $m'(z^i)$

We use the 2 basic relations:

(a) $\prod_{i=1}^{p-1} z^i = (-1)^{p-1}$ (since the solution of $1 + t + \cdots + t^{p-1} = 0$ are z^i, $1 \le i \le p-1$).

(b) $\prod_{i=1}^{p-1} (1 - z^i) = p$; since if $f(t) = t^p - 1$, LHS $= f'(1)$.

Now $\prod_{j \neq i} (z^i - z^j) = z^i \prod_{k \neq 0, -1} (1 - z^k) = \frac{z^i p}{1 - z^{-i}}$ by (b).

Hence $\prod_{i=1}^{p-1} \prod_{j \neq i} (z^i - z^j) = \left(\prod_{i=1}^{p-1} z^i \right) \cdot \frac{p^{p-1}}{\prod_{i=1}^{p-1} 1 - z^i} = (-1)^{p-1} p^{p-2}$ by (a) & (b).

$\therefore D(1, z, \cdots, z^{p-2}) = (-1)^{\frac{1}{2}(p-1)+p-1} p^{p-2} = (-1)^{\frac{p-1}{2}} p^{p-2}$ since p odd. $\square$

ALITER $D = (-1)^{\frac{1}{2}(p-1)(p-2)} N_{K/\mathbb{Q}}(m'(z))$.

Now $m(t) = \frac{t^p - 1}{t - 1}$, so $m'(t) = \frac{p t^{p-1}(t-1) - (t^p - 1)}{(t-1)^2} = \frac{(p-1)t^p - p t^{p-1} + 1}{(t-1)^2}$

$m'(z^i) = \frac{(p-1) - p z^{i(p-1)} + 1}{(z^i - 1)^2} = \frac{p(1 - z^{-i})}{(1 - z^i)^2}$

$\therefore D = (-1)^{\frac{1}{2}(p-1)} \prod_{i=1}^{p-1} p \cdot \frac{(1 - z^i)}{(1 - z^i)^2} = (-1)^{\frac{1}{2}(p-1)} p^{p-1}$ $\square$.

§5 Factorization of integers; Dedekind domains & ideals.

Let A be a ring (int. domain), M an A-module. Recall that the following are equiv.

(a) Each non-empty family of submodules of M has a maximal elt.

(b) M satisfies the ACC on submodules.

(c) Every submodule of M is finitely generated (as A-module).

A module M satisfying (a) (or (b) or (c)) is called Noetherian. We assume basic facts about noetherian modules.

A is a noetherian ring if A is noeth. as A-module.

If A is a ring (comm. with 1) an ideal $\equiv$ an A-submodule.

An ideal $\mathfrak{p} \subsetneq A$ is prime if $A/\mathfrak{p}$ is an int. domain.

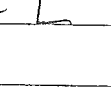
If $\mathfrak{m} \subsetneq A$ is a maximal ideal $A/\mathfrak{m}$ is a field. So maximal $\Rightarrow$ prime. The converse is generally false.

Sums & products of ideals

For ideals $\mathfrak{a}, \mathfrak{b}$, $\mathfrak{a}\mathfrak{b} = \{\sum_{\substack{a_i \in \mathfrak{a} \\ b_i \in \mathfrak{b}}} a_i b_i\} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

For $\mathfrak{p}$ prime, if $\mathfrak{p} \supseteq \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n$ (ideals), then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i. For if not, $\forall i$ have $a_i \in \mathfrak{a}_i \setminus \mathfrak{p}$. Then $\prod a_i \in \mathfrak{p} - \times \prod (a_i + \mathfrak{p}) = 0' \in A/\mathfrak{p}$ ⚡.

Lemma 1. Let A be an integrally closed noetherian ring, K = quot. fld of A, L a deg n ext of K, A' the integral closure of A in L. Then A' is a finitely generated noetherian A-module.



(* because A' f.g. $\Rightarrow A' \leq \frac{A^n}{Q}$.)

Pf. Since A' is a submodule of a f.g. A-module A' is a f.g. module over A, because any f.g. module over a noetherian ring is noetherian* & hence any submodule is noetherian. So A' is noeth as A-module.

On the other hand, any ascending chain of ideals of A' terminates, since ideals are A-modules. Thus A' is a noeth. ring. ∎

(a)

Cor! If L is an alg no. fld, the integers in L form a noetherian ring.

Lemma 2. In a noetherian integral domain A each non-zero ideal contains a product of non-zero prime ideals. (NB A is prime!)

Pf. Suppose false. Then the set Φ of non-zero ideals not containing any non-triv prod of non-zero prime ideals is non-empty, & hence has a max'l elt, say M.

Now M is not prime by hypoth so $\exists\ x, y \in A \setminus M$ st. $xy \in M$. Hence $Ax + M$ & $Ay + M$ both contain M properly & so $\notin \Phi$ both contain products of prime ideals.

Say $Ax + M \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_k$, $Ay + M \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_l$.

Then $(Ax + M)(Ay + M) \supseteq \mathfrak{p}_1 \cdots \mathfrak{q}_l$, so. $M \supseteq \mathfrak{p}_1 \cdots \mathfrak{q}_l$. ∎.

24-8-17.

Lemma 3. Suppose L is an algebraic number field of degree n (over $\mathbb{Q}$) & let A be its ring of integers and $I \neq 0$ an ideal of A. Then I is a free abelian group of rank n. In particular it is finitely generated (over $\mathbb{Z}$).

Pf. Let $a_1, \ldots, a_n$ be an integral basis of A. If $a \in I$, $a \neq 0$, then $aa_1, \ldots, aa_n$ are independent over $\mathbb{Z}$, for if $\sum \lambda_i a a_i = 0$ then $a \cdot \sum \lambda_i a_i = 0$, so $\lambda_i = 0\ \forall i$. Thus $\mathbb{Z}^n \supseteq I \supseteq \mathbb{Z}^n$. Hence $I \cong \mathbb{Z}^n$. ∎

Cor 3'. If, in Lemma 3, I is prime, then I is maximal.

Pf. If I is prime then A/I is an integral domain. But by Lemma 3, A/I is finite, so A/I is a finite integral domain, hence a field. □

[A finite integral domain D is a field: for if $d \in D$, $d \neq 0$, we need only show d has an inverse d' s.t. $dd' = 1$. But multiplication $x \mapsto dx$ is an injective map $: D \to D$ since $dx = dy \iff d(x-y) = 0 \iff x = y$. Hence the map is surjective, & $\exists\, d'$ s.t. $dd' = 1$].

Defn. A Dedekind Domain is a noetherian, integrally closed ring in which every prime ideal is maximal.

Examples. $\mathbb{Z}$; any PID (since in a PID a prime ideal $\mathfrak{p} = aA$ & A/aA is an integral domain. So for $b \in A$, $\notin aA$ $\langle a, b \rangle_A = A$ & hence $\exists\, a', b'$ s.t. $aa' + bb' = 1$ & hence b is invertible mod A).

By Lemma 3, the ring of integers in a number field is a Dedekind domain.

More generally:

Theorem 4. Let A be a Dedekind domain, K = quot fld of A, and $\mathbb{C} \supset L \supset K \supset A$ with $[L:K] = n$. Let A' be the integral closure of A in L. Then A' is a f.g. ($=$ integrally closed) A-module, & is again a Dedekind domain.

Pf. By Thm 6 of §4, A' is a submodule of a free A-module of rank n. Hence A' is a finite noetherian (hence f.g.) A-module. If $I_0 \subset I_1 \subset \cdots$ is an ascending chain of ideals of A', it terminates, since

these are A-submodules. So A' is a noetherian ring.
It RTP that if $\mathfrak{P}'$ is a prime ideal of A', $\mathfrak{P}' \neq 0, A'$, then $\mathfrak{P}'$ is maximal.

Let $\mathfrak{P} = \mathfrak{P}' \cap A$. For any $x \in A'$, we have $A'x \cap A \neq 0$, for x satisfies an equation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, with $a_i \in A$, $a_0 \neq 0$. So $a_0 \in A'x \cap A$. Hence $a_0 \in \mathfrak{P}$, so $\mathfrak{P} \neq 0$. Hence $\mathfrak{P}$ is a non-trivial prime ideal of A (if $a, b \in A$ with $ab \in \mathfrak{P} = \mathfrak{P}' \cap A$, then $a \in \mathfrak{P}'$ or $b \in \mathfrak{P}'$ whence $a \in \mathfrak{P}' \cap A$ or $b \in \mathfrak{P}' \cap A$). Hence $\mathfrak{P}$ is a maximal ideal of A, so $A/\mathfrak{P}$ is a field.

We show $A'/\mathfrak{P}'$ is integral over $A/\mathfrak{P}$

[Note that $\frac{A}{\mathfrak{P}} \cong \frac{A}{A' \cap \mathfrak{P}'} \cong \frac{A + \mathfrak{P}'}{\mathfrak{P}'} \subseteq \frac{A'}{\mathfrak{P}'}$.]

This is clear because if $x + \mathfrak{P}' \in A'/\mathfrak{P}'$ then x satisfies $f(x) = 0$ over $A[x] \Rightarrow x + \mathfrak{P}'$ satisfies $\bar{f}(\bar{x}) = 0$ where $\bar{x} = x + \mathfrak{P}'$ and $\bar{f} = f \bmod \mathfrak{P} \in A/\mathfrak{P}[x]$. ∎

Hence $A/\mathfrak{P}$ a field $\Rightarrow$ $A/\mathfrak{P}'$ is a field (a standard result in integral dependence). □

We have seen that rings of integers in an algebraic

Cor 4' The ring of integers in an algebraic number field is a Dedekind domain.

Pf. Take $A = \mathbb{Z}$, $K = \mathbb{Q}$ in Thm 4. □

Our main interest in Dedekind domains is in how they differ from PID's. This is a historical road block in Fermat's last Thm.

Example. Let $L = \mathbb{Q}(\sqrt{-5})$. Since $-5 \equiv 3 \pmod 4$ the integers in this field are $A = \mathbb{Z}[\sqrt{-5}]$

$$= \{ u + v\sqrt{-5} \mid u, v \in \mathbb{Z} \}.$$

Consider the factorization. Units in A. Suppose $\alpha, \beta \in A$ and $\alpha\beta = 1$. Then $N(\alpha)N(\beta) = 1$. Now

$$N(u + v\sqrt{-5}) = (u + v\sqrt{-5})(u - v\sqrt{-5}) = u^2 + 5v^2$$

$$= 1 \Leftrightarrow u = \pm 1, \quad v = 0.$$

Hence the only units in A are ± 1.

Now consider the factorization

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3.$$

We have $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$, $N(2) = 4$, $N(3) = 9$.

I claim: $1 \pm \sqrt{-5}$, 2, 3 are all irreducible.

For: if $1 + \sqrt{-5} = ab$ then $N(1 + \sqrt{-5}) = 6 = N(a)N(b)$.

If $N(a) = 6$ then $u^2 + 5v^2 = 6 \Rightarrow u = \pm 1$, $v = \pm 1$. So $a = \pm(1 \pm \sqrt{-5})$, ex. $1 - \sqrt{-5} \nmid 1 + \sqrt{-5}$, so $N(a) = 2$ or 3 & there is no $u + \sqrt{-5}v$ with $N = 2$ or 3. So $1 \pm \sqrt{-5}$ is irred.

Similarly 2 is irred. ($N(2) = 4$, so only divisors of 2). Also 3 irred.

Hence $1 \pm \sqrt{-5}$, 2, 3 are irred but not prime.

$\therefore$ A is not a UFD, not a PID but is a DD.

This is why Kummer introduced "ideal numbers". We will show that they form a UFD. Kummer had the basic ideas for analysing integers in cyclotomic fields, but it was Dedekind who did it.

FRACTIONAL IDEALS

Let A be an integral domain, K its quotient field.
A fractional ideal of A (or of K wrt A) is an A submodule $I \subseteq K$ s.t. for some $x \in K$, $I \subset xA$.
[This means that the elts of I have a common denominator

Defn. If I, J are fractional ideals,

$$I + J = \{ i + j \mid i \in I, j \in J \}.$$

$$IJ = \left\{ \sum_{i \in \text{finite}} i_t j_t \;,\; i_t \in I, j_t \in J \right\}.$$

$$I \cap J = \{ a \mid a \in I, a \in J \}.$$

29-8-2017

Ex. Check that these are fractional ideals.

(Hint)

Theorem 5: Let A be a Dedekind domain not a field. In the monoid of fractional ideals, A is the identity, and each fractional maximal ideal M of A is invertible in this monoid; i.e. given M maximal $\exists$ fractional ideal M' s.t. $MM' = A$.

Pf. Let $M' = \{ x \in K \mid xM \subseteq A \}$, where K = qu. fld of A.
Then M' is a fractional ideal since if $d \in M$, $d \neq 0$ then $xd \in A$ $\forall x \in M'$ i.e. $x \in \frac{1}{d} \cdot A$.
Clearly MM' is an ideal of A which contains M, since $1 \in M'$. Thus $M'M = M$ or $M'M = A$.
If $M'M = M$, take $x \in M'$, then $xM \subseteq M$, so $x^2 M \subseteq xM \subseteq M$ etc. So $A[x]M \subseteq M \subseteq A$, and $A[x]$ is a fractional ideal (since $A[x]d \subseteq A$ $\forall d \in M$).
Since A is noetherian, M is f.g. over A;
[hint] if $A[x] \subseteq A$ is an ideal, hence f.g. over A by $d_1, \ldots, d_N$ say.
$\therefore$ $A[x]$ is an A-submodule of $A[f_1, \ldots, f_N]$ — noetherian A-module

Hence x is integral over A, & since A is Dedekind, $x \in A$. It follows that $M' \subseteq A$ & so $M' = A$. We show this is impossible. (using Lemma 2 above).

Let $a \in M$; then $M \supseteq Aa \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$ for primes $\mathfrak{p}_i$ with n minimal. Since $M \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$ it follows that $M \supseteq \mathfrak{p}_i$ some i; say wlog $M \supseteq \mathfrak{p}_1$. Since $\mathfrak{p}_1$ is max'l, it follows that $\mathfrak{p}_1 = M$. Write $a = \mathfrak{p}_2 \cdots \mathfrak{p}_n$.

Then $M \supseteq Aa \supseteq M \cdot a$. But $Aa \neq a$ by the minimality of n. So $\exists\, b \in a$ s.t. $b \notin Aa$, and $M \supseteq Aa \supseteq Mb$. So $M \cdot \frac{b}{a} \subseteq A$, since $\frac{b}{a} \in M'$,

but $b \notin Aa \Rightarrow \frac{b}{a} \notin A$. ✳ Hence $MM' \neq M$, so $MM' = A$. □

DEF A fractional ideal $\subseteq A$ is an integral ideal $\equiv$ ideal of A.

Cor 5 (1) If a is an (integral) ideal — i.e. an ideal of A and $xa \subseteq a$, then $x \in A$. (2) $\mathfrak{p}^{-1} \neq A$ $\forall$ $\mathfrak{p}$ max'l.

Pf. As above, we see $A[x]a \subseteq a \subseteq A$. Hence for $d \in a$, $dA[x] \subseteq A$ & hence $dA[x]$ is an ideal of A & hence f.g. as A-module. Hence $A[x]$ is contained in a f.g. A-module, so x is integral over A & hence $x \in A$. □

(2) If $\mathfrak{p}^{-1} \subseteq A$, then $\mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{p}$ ✳.

[* Since $dA[x]$ generated by $df_1, \ldots, df_N$ $\Rightarrow A[x] \subseteq \sum_{i=1}^{N} A \cdot f_i$]

[NOTE: A fractional ideal is an intersection A-submodule of K = quot. field of A]

Theorem. Let A be a Dedekind domain. Then

(i) Every non-zero fractional ideal $a \neq 0$ can be written essentially uniquely in the form $a = \mathfrak{p}_1^{n_1} \mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_k^{n_k}$ where $\mathfrak{p}_i$ is a prime ideal of A and $n_i \in \mathbb{Z}$.

(ii) The monoid of fractional ideals is a group.

NB it suffices that to prove existence for integral ideals, for if I is fractional, $dI \subseteq A$ & $dI = (dA)I$, so $I = (dA)^{-1} \cdot (dA)I$. □

↖

<u>Proof</u>. (i) <u>Existence</u>. Let Φ be the set of ideals of A not expressible as products of prime (fractional) ideals. If $\Phi \neq \phi$, Φ contains a maximal element B. Let p be a prime ideal of A such that $p \supsetneq B$. Then $p^{-1}B \subseteq p^{-1}p = A$. Moreover since $1 \in p^{-1}$, $p^{-1}B \supseteq B$.

But $p^{-1}B \neq B$ by the argument in the Pf of Thm 5 (*) [If $p^{-1}B = B$, then take $x \in p^{-1}$; then $A[x]B \subseteq B \subseteq A$ & the usual argument shows $A[x]$ is f.g. over A, hence x is i.e. A and so $x \in A$; thus $p^{-1} \subseteq A$. But then, take any $a \in p$. By Lemma 3, $p \supseteq Aa \supseteq p_1 \ldots p_n$ & so $p = p_1$.

Hence $p \supsetneq Aa \supseteq p \mathfrak{B}\mathfrak{C}$, ~~[illegible]~~ X]

$\Rightarrow \exists c \in \mathfrak{C}, c \notin Aa$, but $Aa \supseteq pc$. So $p \cdot \frac{c}{a} \subseteq A$, so $\frac{c}{a} \in p^{-1}$, $c \notin aA$.

Hence $p^{-1}B \supsetneq B$, and therefore $p^{-1}B = p_1^{n_1} \cdots p_k^{n_k}$.

Multiply by p on both sides to get a similar expression for B.

(ii) <u>Uniqueness</u>. Suppose $\prod_i p_i^{n_i} = \prod_i p_i^{m_i}$.

Then $\prod p_i^{k_i} = A$ $(k_i = n_i - m_i)$. Multiplying by appropriate powers of the p_i we get

(†)— $\prod p_i^{k_i'} = \prod q_i^{l_i}$ with $k_i', l_i > 0$.

But then $p_1 \supseteq \prod q_i^{l_i} \Rightarrow p_1 \supseteq q_i$ some $i \Rightarrow p_1 = q_1$ (why). Hence we may cancel factors to get a shorter expression (†). This proves (ii).

(iii) $(\prod p_i^{n_i})^{-1} = \prod p_i^{-n_i}$. □

Cor 6'. If I_1, I_2 are integral ideals such that $I_1 \supseteq I_2$ then $\exists$ an integral ideal X s.t. $I_2 = I_1 X$.

Pf. $X = I_1^{-1} I_2 \subseteq I_1^{-1} I_1 \subseteq A$. □

Thus: If I_1, I_2 are integral ideals s.t. $I_1 \supseteq I_2$, then $I_1 | I_2$

(*) $p^{-1}B \neq B$, for if $p^{-1}B = B$, then $\forall x \in p^{-1}$, $xB \subset B \subseteq A$. So $x \in A$ by Cor 5'. But $p^{-1} \not\subseteq A$ by the proof of Thm 5. So $p^{-1}B \supsetneq B$, so $p^{-1}B \notin \Phi$.

Cor 6'' Each integral ideal of A divides some principal ideal.

Pf. If $I \trianglelefteq A$ and $a \in I$, then $aA \subseteq I$. Hence in the factorisation of these ideals into products of primes, aA has additional factors, i.e. $I \mid aA$. □

[NB: If J_1, J_2 are two fractional ideals, we always have $J_2 = J_1 \cdot \prod \mathfrak{p}_i^{n_i}$. If $n_i \geq 0 \ \forall i$ then $\prod \mathfrak{p}_i^{n_i}$ is an integral ideal, & conversely. We say $J_1 \mid J_2$ if $J_2 = J_1 I$, with I an integral ideal.]

Cor 6''' In Thm 6, let a be a fractional ideal, with $a = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$. Then $a \subseteq A \iff n_i \geq 0 \ \forall i$.

Proof. $n_i \geq 0 \ \forall i \Rightarrow a \subseteq A$.
Conversely if $a \in A$, $a = \prod_{\text{coprime}} \mathfrak{p}_i^{n_i} \cdot \prod_j \mathfrak{p}_j^{-m_j}$. Since $\mathfrak{p}_j^{-1} \supsetneq 1$, it suffices to show that for any ideal $B \trianglelefteq A$, and prime ideal $\mathfrak{p}$ of A, $B\mathfrak{p}^{-1} \not\subseteq A$.
Assume $B\mathfrak{p}^{-1} \subseteq A$. Then by Cor 5', if $x \in \mathfrak{p}^{-1}$, $Bx \subseteq A$ so $x \in A$. Hence $\mathfrak{p}^{-1} \subseteq A$. But this contradicts the def of Thm 6 (*), hence $B\mathfrak{p}^{-1} \not\subseteq A$. □.

[Pf: If $\mathfrak{p}^{-1} \subseteq A$, then for $a \in \mathfrak{p}$, $\mathfrak{p} \supseteq Aa \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$ for primes $\mathfrak{p}_i$ with n minimal. Hence $\mathfrak{p} \supseteq \mathfrak{p}_i$ some i, & wlog $i=1$. So $\mathfrak{p} \supseteq Aa \supseteq \mathfrak{p} B$, $B = \mathfrak{p}_2 \cdots \mathfrak{p}_n$, $Aa \not\supseteq B$. Take $b \in B \setminus Aa$; then $\mathfrak{p} \supseteq Aa \supseteq \mathfrak{p} b$ & hence $\mathfrak{p} \cdot \frac{b}{a} \subseteq A$, so $\frac{b}{a} \in \mathfrak{p}^{-1} \subseteq A \Rightarrow b \in aA$ ✱]

$a \subseteq B \iff B \mid a$. (Integral ideals).
$(\mathfrak{p}^{-1} \supseteq A)$.

The fractional ideals form a group, which we denote by $I(A)$.
A fractional ideal I is principal if $I = aA$, for some $a \in K$.
Note that the product of 2 principal ideals is principal and the inverse $(aA)^{-1} = a^{-1}A^{-1} = a^{-1}A$, is also principal.
The principal ideals therefore form a subgroup $P(A)$ of $I(A)$.

Definition (i) The class group of A, denoted $C(A)$ is $I(A)/P(A)$. Its elements are called ideal classes.

(ii) An ideal class is a coset of $P(A)$ in $I(A)$.

Note $C(A) = 1 \iff A$ is a PID.

Pf. $C(A) = 1 \Rightarrow$ each fractional ideal is principal so in particular each integral ideal is principal so A is a PID.

If A is a PID and I is a fractional ideal, then $I \subseteq \frac{a}{b}A$, some $a, b \in A$. Hence bI is an ideal of A, so we have $bI = cA$, some $c \in A$. So $I = \frac{cA}{b}$. □

By Thm 6, we may speak of the gcd & lcm of integral ideals

If $I = \prod \mathfrak{p}_i^{n_i}$, $J = \prod \mathfrak{p}_i^{m_i}$

$$\gcd(I,J) = \prod \mathfrak{p}_i^{\min(n_i,m_i)} = I + J.$$
$$\operatorname{lcm}(I,J) = \prod \mathfrak{p}_i^{\max(n_i,m_i)} = I \cap J.$$

We have $(I+J)(I\cap J) = IJ$.

Cor 6(iv) Every integral ideal $\mathfrak{a}$ is the gcd of two principal ideals.

Pf. Cor 6" says that $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$. Then $\mathfrak{a} = \gcd(aA, \mathfrak{b})$ for $\mathfrak{b} = \prod \mathfrak{p}_i^{m_i}$ with $m_i \le n_i \ \forall i$.

Hence $\forall i$, $\exists\, a_i \in \mathfrak{p}^{n_i}$, $a_i \notin \mathfrak{p}^{n_i+1}$. Let $b \in A$ be such that $b \equiv a_i \bmod \mathfrak{p}_i^{n_i+1}$ $\forall i$. ($\exists b$ by Chinese Remainder Theorem). We then have $bA = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k} \times$ (other prime ideals).
$\therefore \gcd(aA, bA) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k} = a$, since
$\mathfrak{p} \mid bA \iff bA \subseteq \mathfrak{p}$. So $\mathfrak{p} \mid aA \Rightarrow \mathfrak{p} = \mathfrak{p}_i$, some i, and $\mathfrak{p}^k \mid bA \in bc\mathfrak{p}^k$. ☐

Chinese remainder theorem. Let $a_1, \dots, a_s$ be relatively prime (in pairs). Then given $a_1, \dots, a_s \in A$, $\exists\, x \in A$ s.t. $x \equiv a_i \bmod a_i$ $\forall i$, & x is unique mod $a_1 \cdots a_s$.

Pf (Ex) We show $\exists\, e_i \in A$ such that $e_i \equiv 1 \bmod a_i$ and $e_i \equiv 0 \bmod a_j$, $j \neq i$. Let $B_i = a_1 \cdots \hat{a}_i \cdots a_s$, then $(B_i, a_i) = (1)$, i.e. $a_i + B_i = 1$. Hence $\exists\, x_i \in a_i$, $e_i \in B_i$ s.t. $x_i + e_i = 1$.

[NB, $\gcd(a, B) = 1 \iff a + B = A$.
If $a + B \neq A$, $a + B = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$. So $\mathfrak{p}_1^{-1} a + \mathfrak{p}_1^{-1} B \subseteq A$, which is impossible, since $\mathfrak{p}_1^{-1} a \notin A$ & $\mathfrak{p}_1^{-1} B \notin B$, since $\mathfrak{p}^{-1} I \subseteq A \iff \mathfrak{p} \mid I$]

Uniqueness $x \equiv y = a_i \ \forall i \iff (x - y) \in a_i \ \forall i \Rightarrow x \equiv y \bmod \prod a_i$. ☐

~~The class group of an algebraic number field - Minkowski's theorem~~

NOTE. $\gcd(a, B) = A$ (ideals)
$\iff a + B = A$
For. If $a + B = A$ & $\mathfrak{p} \mid a$, $\mathfrak{p} \mid B$, then $\mathfrak{p} \mid A$ ✕.
Conversely if $\gcd(a, B) = A$, and $a + B \subseteq \mathfrak{p}$, then $\mathfrak{p} \mid a$, $\mathfrak{p} \mid B$. ☐

§6 The Class Group of an algebraic number field – Minkowski's Theorem.

In this section K will be an algebraic number field of degree n, and A its ring of integers. The main objective is to prove that the class group is finite (remember: it is trivial if A is a PID). The method of proving this is to plunge the integers ($\simeq \mathbb{Z}^n$) into Euclidean space as a lattice and to look at the volumes of ideals. We shall show that each ideal class (i.e. coset of the principal ideals) contains an ideal of rather small volume and since there are only finitely many (ideals) of a given volume, this will prove finiteness.

As a first step towards the "volume" of an ideal, we make the following defn.

Defn. The norm $N(\mathfrak{a})$ of an ideal $\mathfrak{a} \subseteq A$ is $|A/\mathfrak{a}|$.

(Recall this is finite from Lemma 5.3).

Lemma 1 If $x \in A$, $N_{K/\mathbb{Q}}(x) = N(Ax)$.

Pf. Take an integral basis $b_1, \dots, b_n$ of A.
Then by the elementary divisor theorem, Ax has basis $\kappa_1 b_1, \dots, \kappa_n b_n$ (possibly after changing $b_1, \dots, b_n$).
Hence with these bases, x has matrix $\begin{pmatrix} \kappa_1 & & \\ & \ddots & \\ & & \kappa_n \end{pmatrix}$.

But Ax has basis $b_1 x, \dots, b_n x$
($\because x = \left(\sum \lambda_i b_i\right) x$ for some λ_i $\because \sum \lambda_i b_i x = 0 \Rightarrow \sum \lambda_i b_i = 0 \Rightarrow \lambda_i = 0 \; \forall i$)
Hence $\exists$ unimodular $U \in GL_n(\mathbb{Z})$ s.t. $U M_x = \begin{pmatrix} \kappa_1 & & \\ & \ddots & \\ & & \kappa_n \end{pmatrix}$ so
$\det M_x = \kappa_1 \cdots \kappa_n$.

But $A/\mathfrak{a} \cong \dfrac{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}{\kappa_1\mathbb{Z} \oplus \kappa_2\mathbb{Z} \oplus \cdots} \cong \dfrac{\mathbb{Z}}{\kappa_1\mathbb{Z}} \oplus \cdots \oplus \dfrac{\mathbb{Z}}{\kappa_n\mathbb{Z}}$.

So $N(a) = \prod_{i=1}^{n} k_i = |N_{K/\mathbb{Q}}(x)|$ □.

Thm 3.9-13.

Lemma 2 For any two non-zero integral ideals $a, B \trianglelefteq A$, we have $N(aB) = N(a)N(B)$.

Pf. Since B is a product of prime (maximal) ideals, it suffices to take $B = \mathfrak{p}$, prime.

$A \supseteq a \supseteq a\mathfrak{p}$.

Now $A/a \cong \dfrac{A/a\mathfrak{p}}{a/a\mathfrak{p}}$ (3rd isom thm).

Hence taking cardinalities, $N(a) = |A/a| = \dfrac{N(a\mathfrak{p})}{|a/a\mathfrak{p}|}$,

i.e. $N(a\mathfrak{p}) = N(a) \cdot |a/a\mathfrak{p}|$.

Observe that $a/a\mathfrak{p}$ is an A-module, which is annihilated by $\mathfrak{p}$. Hence $a/a\mathfrak{p}$ is an $A/\mathfrak{p}$-module i.e. a vector space over the field $A/\mathfrak{p}$.

~~But any subspace of $a/a\mathfrak{p}$ corresponds to an ideal B such that $a \supseteq B \supseteq a\mathfrak{p}$. Since $a\mathfrak{p}$ is maximal in a, $B = a$ or $B = a\mathfrak{p}$ so $\dim_{A/\mathfrak{p}}(a/a\mathfrak{p}) = 1$.~~
~~So $|a/a\mathfrak{p}| = |A/\mathfrak{p}| = N(\mathfrak{p})$.~~

But any subspace of $a/a\mathfrak{p}$ corresponds to an ideal B such that $a \supseteq B \supseteq a\mathfrak{p}$. By looking at the prime decomposition of B one sees that $B \mid a$, $\mathfrak{p}a \mid B$. So $B = a$ or $B = \mathfrak{p}a$. Hence $a/a\mathfrak{p}$ has no proper subspaces & hence $|a/a\mathfrak{p}| = |A/\mathfrak{p}| = N(\mathfrak{p})$.

So $N(a\mathfrak{p}) = N(a)N(\mathfrak{p})$. □

Note that the norm of an ideal becomes larger as the ideal becomes smaller. So norm "=" "inverse" of volume. We next relate this "volume" to the discriminant.

Lemma 3 Suppose $x_1, \dots, x_n$ is an integral basis of K & $a_1, \dots, a_n$ is a basis of $\mathfrak{a}$. Then

$$N(\mathfrak{a}) = \left| \sqrt{\frac{\Delta_{K/\mathbb{Q}}(a_1, \dots, a_n)}{\Delta_{K/\mathbb{Q}}(x_1, \dots, x_n)}} \right| = \left| \sqrt{\frac{\Delta(a_1, \dots, a_n)}{d}} \right|.$$

where $d = \Delta(K)$ is the discriminant of K.

Proof. Let $a_i = \sum_{j=1}^{n} n_{ij} x_j \quad (i = 1, \dots, n)$.

Then $\Delta(a_1, \dots, a_n) = (\det(n_{ij}))^2 \, \Delta(x_1, \dots, x_n)$. (*)

But $N(\mathfrak{a}) = |\det(n_{ij})|$, so

$$N(\mathfrak{a})^2 = \frac{\Delta(a_1, \dots, a_n)}{\Delta(x_1, \dots, x_n)}. \qquad \square$$

[(*) follows because $\exists$ a basis $b_1, \dots, b_n$ of A such that $k_1 b_1, \dots, k_n b_n$ is a basis of $\mathfrak{a}$.

$\therefore \exists$ unimodular matrices (in $GL_n(\mathbb{Z})$) U_1, U_2

s.t. $(b_1 \cdots b_n) = (x_1 \cdots x_n) U_1$ (x_i) basis of A

$(k_1 b_1, \dots, k_n b_n) = (a_1 \cdots a_n) U_2$ (a_i) basis of $\mathfrak{a}$.

So $(a_1 \cdots a_n) = (b_1 \cdots b_n) D U_2^{-1}$ $\quad D = \mathrm{diag}(k_i)$

$= (x_1 \cdots x_n) U_1 D U_2^{-1}$

so $N(\mathfrak{a}) = |\det(U_1 D U_2^{-1})| = |\det(U_1 D U_2^{-1})| = \left| \prod k_i \right|$]

We will show that the class number of K is finite by showing that every ideal class has contains an integral ideal of small norm. We also show that only finitely many ideals have norm $\leq B$ (B fixed), which proves the result.

Lemma (Observation). For any ideal $a \leq A$, a divides $N(a)$ (i.e. $a \mid N(a)A$).

Pf. $|A/a| = N(a)$. So A/a is an abelian group of order $N(a)$, whence $N(a) \cdot \frac{A}{a} = 0$, ie $N(a)A \subseteq a$. Hence $a \mid N(a)A$. □.

Hence: If $\mathfrak{p}$ is a prime ideal, $\frac{A}{\mathfrak{p}}$ is a field & hence has p^e elements where p is a rational prime, so $\mathfrak{p} \mid p^e A$.

Proposition 4. Given an algebraic number field K there is a constant γ (to be determined later) such that any integral ideal $a \neq 0$ contains a non-zero element x s.t.

$$|N_{K/\mathbb{Q}}(x)| \leq \gamma \sqrt{d}\, N(a),$$

where d = discriminant of K.

$$\gamma = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}$$

Pf: We postpone the proof, which will depend on several intermediate results.

Corollary of Lemma above. Every ideal class contains an integral ideal.

Pf. Write $[a]$ for the ideal class of a. Now any ideal $a = \mathfrak{B}\mathfrak{C}^{-1}$ where $\mathfrak{B}, \mathfrak{C}$ are integral. By the Lemma (Observation) $(N(\mathfrak{C})) = \mathfrak{C}\mathfrak{D}$ so $\mathfrak{C}^{-1} = \mathfrak{D} \cdot (N(\mathfrak{C}))^{-1}$

$\therefore a = \mathfrak{B}\mathfrak{C}^{-1} = \mathfrak{B}\mathfrak{D}(N(\mathfrak{C}))^{-1}$ & so $[a] = [\mathfrak{B}\mathfrak{D}]$, & $\mathfrak{B}\mathfrak{D}$ is integral.

□.

Theorem 5 (Ideal class theorem)
The number of ideal classes of an algebraic number field is finite — i.e. its class group is a finite abelian group.

Proof of Thm 5, given Prop 4.
Let c be an ideal class and take any integral ideal a in c^{-1}. [such always exists by the one above].
Choose $x \in a$ as in Proposition 4. Since $x \in a$, $xA \subseteq a$, so $a \mid xA$ & so $\exists$ an integral ideal $\mathfrak{B}$ s.t. $xA = a\mathfrak{B}$.

$$N(a)\,N(\mathfrak{B}) = N(xA) = N(x) \leq \gamma\sqrt{d}\; N(a).$$

$$\therefore N(\mathfrak{B}) \leq \gamma\sqrt{d}.$$

But $a\mathfrak{B} = (x)A$ is principal, so $[\mathfrak{B}] = [a^{-1}] = c$, since $a \in c^{-1}$. Hence $\exists$ an integral ideal $\mathfrak{B} \in c$ with $N(\mathfrak{B}) \leq \gamma\sqrt{d}$.

Further, a fixed integer m has only finitely many prime (ideal) divisors since $mA = \prod \mathfrak{p}_i^{n_i}$. Hence there is only a finite number* of integral ideals $\mathfrak{B}$ with $N(\mathfrak{B}) \leq \gamma\sqrt{d}$. Since each ideal class contains at least one such, there are just finitely many ideal classes. [we have an injection map $\{c\} \to \{\mathfrak{B} = \text{int ideals with norm} < \gamma\sqrt{d}, \text{ a finite set}\}$] □.

It therefore remains to prove Proposition 4. This will be done by putting K into a metric setting, and for this we need to separate real & complex coordinates.

* [Crucial argument: If $N(\mathfrak{B}) = m$, then $\mathfrak{B} \mid mA$. But mA has only finitely many divisors, hence there are only finitely many $\mathfrak{B}$ with $\mathfrak{B} \mid mA$ & hence only finitely many $\mathfrak{B}$ with $N(\mathfrak{B}) = m$, hence only finitely many $\mathfrak{B}$ with $N(\mathfrak{B}) \leq m$.]

Suppose $K = \mathbb{Q}(y)$ and y has min polynomial $m(t)$. Since $m(t) \in \mathbb{Q}[t]$, its roots occur either real, or come in conjugate pairs of complex conjugates.

The roots of $m(t)$ which in $\mathbb{C}$ may therefore be written as follows:

$[y_1, \cdots, y_{r_1}]$ real roots.

$[y_{r_1+1}, \cdots, y_{r_1+r_2}]$ complex roots.

$[y_{r_1+r_2+1}, \cdots, y_{r_1+2r_2}]$ where $y_{r_1+r_2+i} = \overline{y_{r_1+i}}$.

Then $r_1 + 2r_2 = n = \deg m(t)$.

Let $\sigma_1, \cdots, \sigma_n$ be the distinct $\mathbb{Q}$ imbeds $: K \hookrightarrow \mathbb{C}$, defined by $\sigma_i(y) = y_i$.
Then $\sigma_i(K) \subseteq \mathbb{R}$ for $i = 1, \cdots, r_1$ and
$\sigma_j(K) = \overline{\sigma_{j+r_2}(K)}$ if $r_1 + 1 \leq j \leq r_1 + r_2$.

Since the last r_2 σ_i's are determined by the previous r_2, we may define a monomorphism of abelian groups

$$\sigma : K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \approx \mathbb{R}^n \quad \text{by}$$

$$\sigma(x) = (\sigma_1(x), \cdots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \cdots, \sigma_{r_1+r_2}(x)).$$

To understand σ we need to study subgroups of $\mathbb{R}^n$.

$\sigma(A)$

Defn. A (closed) subgroup of $\mathbb{R}^n$ is *discrete* if it intersects with each compact subset of $\mathbb{R}^n$ in a finite set. [Eg $\mathbb{Z}^n$.
($\Leftrightarrow$ it is discrete in the subspace topology).

Theorem 6. If H is a discrete subgroup of $\mathbb{R}^n$, then H is generated as a group by r linearly indept elements of $\mathbb{R}^n$, where $r \leq n$.

Proof Choose a maximal set of $\mathbb{R}$-linearly indept elts $e_1, \dots, e_r$ of H. Define the parallelepiped $P = \{\sum_{i=1}^{r} \alpha_i e_i \mid 0 \leq \alpha_i < 1\}$. Then P is compact & hence contains just a finite number of points of H.

If $x = \sum \lambda_i e_i$ is any point of H, define for $k \in \mathbb{Z}$
$x_k = kx - \sum [k\lambda_i] e_i$ where $[\alpha]$ = integral part of α.
Then $x_k \in P \cap H$ (for $kx \in H$ & $\sum e_i \in H \ \forall s \in \mathbb{Z}$). So there are only finitely many distinct x_k.

If $x_k = x_\ell$, then $(k-\ell)\lambda_i = -[k\lambda_i] + [\ell\lambda_i]$
(since the e_i are linearly indept). Hence $\lambda_i \in \mathbb{Q}$.
Further, the maximality of $\{e_i\}$ implies that each elt of H is a $\mathbb{Q}$-linear combination of the e_i. So the e_i generate H over $\mathbb{Q}$.

But $x = x_1 + \sum [\lambda_i] e_i$, where $x_1 \in P \cap H$.
Hence H is generated over $\mathbb{Z}$ by the finite set $P \cap H \cup \{e_1, \dots, e_r\}$. Hence H is generated by a finite set of $\mathbb{Q}$-linear combinations of the e_i.

It follows that $dH \subseteq \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$.
$\therefore H$ is a subgroup of the f.a.g. $\mathbb{Z}\frac{e_1}{d} + \cdots + \mathbb{Z}\frac{e_r}{d}$.
Hence H is a fag of rank r. $\square$.

Example. A point $x = (\theta_1, \dots, \theta_n)$ with some θ_i irrational generates, with $e_1, \dots, e_n$ (standard basis of $\mathbb{R}^n$), a non-discrete subgroup H. Hence 0 is a limit point of elts of H, because one $\exists$ nbd which is such a limit point & we can take $h = 0$ by translation. Hence for each $\varepsilon > 0$, $\exists$ integers $q \neq 0$ and p_i s.t.

$$\left| qx - \sum_1^n p_i e_i \right| < \varepsilon \quad \text{i.e.} \quad |q\theta_i - p_i| < \varepsilon \quad \forall i.$$

i.e. $\left|\theta_i - \frac{p_i}{q}\right| < \frac{\varepsilon}{q}$, which is interesting (better approx^n than for $(x \bmod q)$. [This was merely the fact that any nbd of 0 contains infinitely many pts of H.]

If a discrete subgroup of $\mathbb{R}^n$ has rank n, it is called a lattice. If $H = \langle e_1, \dots, e_n \rangle$ then by the proof of Thm 6, $P = \{\sum_{i=1}^n \alpha_i e_i \mid 0 \le \alpha_i < 1\}$ is a fundamental domain for H in the sense that each element of $\mathbb{R}^n$ can be moved by H into precisely one point of P. Fundamental domains usually are required to be connected, as this one is.

Let μ denote Lebesgue measure (Haar measure) on $\mathbb{R}^n$. Then H preserves volume (it is a group of translations). And $|\mathbb{R}^n / H| = \mu(P_e)$, because if $b_1, \dots, b_n$ is an orthon. basis of $\mathbb{R}^n$ and $e_i = \sum \lambda_{ij} b_j$, then $\mu(P) = |\det \lambda_{ij}|$.

Hence $\mu(P_e)$ is indept of basis, & we write $\mu(P) = \text{volume}(\mathbb{R}^n / H)$.

P_e = Lattice with basis $e = (e_1, \dots, e_n)$.

In Prop 4, we prove that, $\boxed{\gamma = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}}$

Theorem 7. (Minkowski's convex body theorem).
Let S be a convex subset of $\mathbb{R}^n$ which is symmetric about 0 (i.e. $s \in S \Rightarrow -s \in S$). If $\mu(S) > 2^n \mu(\mathbb{R}^n/H)$ then S contains a point of H.

Pf. Consider $S' = \frac{1}{2}S = \{\frac{1}{2}x \mid x \in S\}$; evidently $\mu(S') > \mu(\mathbb{R}^n/H)$. Now the canonical map $\eta: S' \to \mathbb{R}^n/H$ is locally volume preserving. Hence the volume condition implies that $\exists\, x, y \in S'$, $x \neq y$, such that $\eta(\frac{x}{2}) = \eta(\frac{y}{2})$, i.e. $\frac{1}{2}(x-y) \in H$.

But $x \in S$, $-y \in S \Rightarrow \frac{1}{2}x + \frac{1}{2}(-y) \in S \cap H$. □.

Cor 7'. If in Thm 7 $\mu(S) = 2^n \mu(\mathbb{R}^n/H)$ and S is compact (i.e. closed because it must be bounded) then $S \cap H \neq \phi$.

Proof By Thm 7, $(1+\varepsilon)S$ contains an elt of H $\forall\, \varepsilon > 0$. But the compact set $(1+\varepsilon)S$ contains only finitely many elts of H so there is one which is closest to the origin lies in S.

For if $h_1, \dots, h_\ell$ are these elements, let $\delta_i = \inf\{\varepsilon \mid h_i \in (1+\varepsilon)S\}$. If $\delta_i = 0$ some i, then $h_i \in S$, since $h \in \bar{S} \Rightarrow h \in S$. Otherwise if $\delta_i > 0$ $\forall\, i$, take $\delta < \delta_i$ $\forall i$, then $(1+\delta)S \cap H = \phi$. ※ □.

GO TO P50

We now turn to the

Proof of Prop. 4.
We shall show that $\exists$ constant $\gamma = \gamma(n)$ s.t. for any integral ideal $\mathcal{A}$, $\exists\, x \in \mathcal{A}$ with $|N(x)| \leq \gamma\, \mathrm{Nat}\, N(\mathcal{A})$.

In fact we shall show that γ can be taken to be $\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}$

Now for any $x \in K$, we have

$$|N(x)| = \prod_{i=1}^{n} |\sigma_i(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2$$

Now recall the arithmetic-geometric mean inequality:

(*) Let $a_1, \dots, a_n \in \mathbb{R}$, $a_i \geq 0$ $\forall i$. Then

$$a_1 \cdots a_n \leq \left(\frac{a_1 + \cdots + a_n}{n}\right)^n$$

Apply this with $a_i = |\sigma_i(x)|$, we get:

$$|N(x)| \leq \left(\frac{1}{n}\left(\sum_{i=1}^{r_1} |\sigma_i(x)| + 2\sum_{i=r_1+1}^{r_1+r_2} |\sigma_i(x)|\right)\right)^n$$

Hence if $y = y_1, \dots, y_{r_1}, y_{r_1+1}, \dots, y_{r_1+r_2} \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ we define $\delta(y) = \sum_{1}^{r_1} |y_i| + 2\sum_{r_1+1} |y_j|$, and further define

$$S_r = \{y \in \mathbb{R}^n \mid \delta(y) \leq r\} \qquad (r > 0).$$

Then S_r is evidently a convex subset of $\mathbb{R}^n$ for if $y, y' \in \mathbb{R}^n$, and $t \in [0,1]$, define $y(t) = ty + (1-t)y'$.

Then $|y(t)_i| = |ty_i + (1-t)y_i'| \leq t|y_i| + (1-t)|y_i'|$, whence

$$\delta(y(t)) \leq t\delta(y) + (1-t)\delta(y') \leq r \text{ if } \delta(y) \leq r,\ \delta(y') \leq r.$$

Thus S_r is a convex compact subset of $\mathbb{R}^n$. Moreover we shall later do an integral computation to show that

$$(**) \quad \mu(S_r) = V(r) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{r^n}{n!}$$

[We don't really need to know the precise value of $V(r)$.]

Now take an ideal $\mathfrak{a} \subseteq A$.

Choose r so that $\mu(\mathcal{S}_r) = 2^n \mu(\mathbb{R}^n / \sigma(\mathcal{A}))$. Then by Cor 7', ...

Now return to the situation of the number field K, with ring of integers A, and $[K:\mathbb{Q}] = n = r_1 + 2r_2$.

Lemma 8. Suppose M is a free $\mathbb{Z}$-submodule of K of rank n, with ($\mathbb{Z}$-) basis $x_1, \dots, x_n$. Then $\sigma(M)$ is a lattice in $\mathbb{R}^n$ with $\mu(\mathbb{R}^n / \sigma(M)) = 2^{-r_2} |\det \sigma_i(x_j)|$.

Proof. $\sigma(M)$ is generated by $\sigma(x_1), \dots, \sigma(x_n)$; we wish to show that the $\sigma(x_i)$ are linearly indpt (over $\mathbb{R}$).
We have $\sigma(x_i) = (\sigma_1(x_i), \dots, \sigma_{r_1}(x_i), \mathrm{Re}(\sigma_{r_1+1}(x_i)), \mathrm{Im}(\sigma_{r_1+1}(x_i)), \dots)$.
Hence if C is the matrix $(\sigma_i(x_j))$ over $\mathbb{C}$, then since

$$\begin{pmatrix} \mathrm{Re}\,\sigma_{r_1+i}(x_j) & \mathrm{Im}\,\sigma_{r_1+i}(x_j) \\ \mathrm{Re}\,\sigma_{r_1+i}(x_{j+1}) & \mathrm{Im}\,\sigma_{r_1+i}(x_{j+1}) \end{pmatrix} = \begin{pmatrix} \sigma_{r_1+i}(x_j) & \sigma_{r_1+r_2+i}(x_j) \\ \sigma_{r_1+i}(x_{j+1}) & \sigma_{r_1+r_2+i}(x_{j+1}) \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2i} & -\frac{1}{2i} \end{pmatrix}$$

(last an orthon. basis of $\mathbb{R}^2$).

It follows that the coeff matrix corresponding to the set $\sigma(x_1), \sigma(x_2), \dots, \sigma(x_n)$ is obtained from C by multiplying by $\left(\begin{smallmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2i} & -\frac{1}{2i} \end{smallmatrix}\right)^{\otimes r_2}$; since $\left|\det \begin{pmatrix} \sigma_1(x_1) \\ \sigma_1(x_n) \end{pmatrix}\right| = \frac{1}{2^{r_2}} |\det C|$. ☐

Cor 8' If A is the ring of integers of K and $\mathcal{A}$ an integral ideal, then $\mu(\mathbb{R}^n / \sigma(A)) = 2^{-r_2} |d|^{\frac{1}{2}}$
and $\mu(\mathbb{R}^n / \sigma(\mathcal{A})) = 2^{-r_2} |d|^{\frac{1}{2}} N(\mathcal{A})$.

Proof. We have seen that $d = \det(\sigma_i(x_j))^2$ if $x_1, \dots, x_n$ is an integral basis. Hence by Lemma 8,
$\mu(\mathbb{R}^n / \sigma(A)) = 2^{-r_2} \sqrt{|d|}$.

* Just point out if $z = x+iy$, $(x\ y) = (z\ \bar{z}) \left(\begin{smallmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2i} & -\frac{1}{2i} \end{smallmatrix}\right)$.

Since $\sigma : A \to \sigma A \subseteq \mathbb{R}^n$ is an isomorphism (i.e. a monomorphism into $\mathbb{R}^n$) and $\mathfrak{a}$ is a subgroup of A of index $N(\mathfrak{a})$, it follows that $\mu(\mathbb{R}^n/\sigma(\mathfrak{a})) = N(\mathfrak{a})\,\mu(\mathbb{R}^n/A)$. □

Proof of Prop 4. Recall: we wish to show that $\exists$ constant $\gamma = \gamma(n)$ s.t. for any integral ideal $\mathfrak{a}$, $\exists\, x \in \mathfrak{a}$ with $|N(x)| \le \gamma\, |d|^{\frac{1}{2}}\, N(\mathfrak{a})$.

[In fact we'll show later that γ may be taken to be $\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}$]

Now for $x \in K$, $|N(x)| = \prod_{i=1}^{n} |\sigma_i(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(x)|^2$

Now for real numbers $a_1, \dots, a_n$ s.t. $a_i \ge 0$, we have
$\prod a_i \le \left(\frac{1}{n}\sum a_i\right)^n$ (geometric/arithm mean).

$$\therefore |N(x)| \le \left[\frac{1}{n}\left(\sum_{1}^{r_1} |\sigma_i(x)| + 2\sum_{r_1+1}^{r_1+r_2} |\sigma_i(x)|\right)\right]^n$$

For $y = (y_1, \dots, y_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ define $\delta(y) = \sum_{1}^{r_1} |y_i| + 2\sum_{r_1+1}^{r_1+r_2} |y_i|$

and let $S_r = \{ y \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n \mid \delta(y) \le r \}$.

Then S_r is a symmetric, compact convex subset of $\mathbb{R}^n$.
To see convexity, let $y, y' \in S_r$ and $t \in [0,1]$. Define $y(t) = ty + (1-t)y'$. Then $y(t)_i = t y_i + (1-t) y'_i$ whence $|y(t)_i| \le t|y_i| + (1-t)|y'_i|$. Hence $\delta(y(t)) \le t\delta(y) + (1-t)\delta(y')$.
Hence if $y, y' \in S_r$, $y(t) \in S_r$ $\forall\, t$.

It is evident that $\mu(S_r) = c r^n$, $c = c(r_1, r_2)$.
[In fact $c = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{1}{n!}$].

Now choose r so that $\mu(S_r) = cr^n = 2^n \mu(\mathbb{R}^n/\sigma(\mathcal{O}))$.

Then $\mu(\mathbb{R}^n/\sigma(\mathcal{O})) = 2^{-r_2}|d|^{\frac{1}{2}} N(\mathfrak{a})$ by Cor 8' $\Rightarrow$

$r^n = \frac{1}{c} \cdot 2^{n-r_2}\sqrt{|d|}\, N(\mathfrak{a})$.

By Cor 7', $\exists\ x \in \mathfrak{a}$, with $\Lambda S(\sigma(x)) \leq r$ ($\sigma(x) \in \sigma(\mathfrak{a}) \cap S_r$, i.e.)

Then for this x, we have

$$|N(\mathfrak{a})| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{r_1+1}^{r_1+r_2} |\sigma_i(x)|^2$$

$$\leq \left(\frac{1}{n} S(\sigma(x))\right)^n, \text{ i.e.}$$

$$\leq \left(\frac{r}{n}\right)^n, \quad r^n = \frac{2^{n-r_2}}{c}\frac{|d|^{\frac{1}{2}}}{n^n} N(\mathfrak{a}).$$

i.e. $\leq \gamma |d|^{\frac{1}{2}} N(\mathfrak{a})$, where $\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \leq$

$$\gamma = \frac{2^{n-r_2}}{c\, n^n} = \frac{2^{n-r_2}}{n^n} \cdot \frac{n!}{2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}} = \frac{2^{n-r_1}\, n!}{n^n \pi^{r_2}} \quad \square.$$

Cor 8' (of ideal class thm). $\exists$ an ideal $\mathfrak{B}$ in $[\mathfrak{a}]$ with $|N(\mathfrak{B})| \leq \gamma |d|^{\frac{1}{2}}$

The next corollaries depend on the fact that γ may be taken to be $\gamma = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}$. We therefore prove this now

Cor 4' For K of degree $n \geq 2$, we have

$d \geq \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1}$. Further $\exists$ const k s.t.

$\frac{n}{\log|d|} \leq k \quad \forall n$.

Proof. From Cor 4', $\exists$ an ideal a with $1 \le N(a) \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|}$

$\Rightarrow \sqrt{|d|} \ge \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{r_2}$ & so $|d| \ge \frac{n^{2n}}{n!^2} \left(\frac{\pi}{4}\right)^n := a_n$.

Now $\frac{a_{n+1}}{a_n} = \frac{(n+1)^{2(n+1)}}{(n+1)!^2} \cdot \left(\frac{\pi}{4}\right) \Big/ \frac{n^{2n}}{(n!)^2}$

$= \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} \ge \frac{3\pi}{4}$

$\therefore |d| \ge \frac{\pi}{4} \cdot \left(\frac{3\pi}{4}\right)^{n-1}$

$\log |d| \ge (n-1) \log \frac{3\pi}{4}$ □

Cor 4'' (Hermite - Minkowski Thm).

$d=1 \Rightarrow K = \mathbb{Q}$.

This follows directly from Cor 4''.

Integral calculation: Compute: $\mu(S_t)$ $\in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$

Proposition (VII) Let $S_t = \{(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \mid \sum_1^{r_1} |y_i| + 2\sum_1^{r_2} |z_i| \le t\}$

Then $\mu(S_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}$

Proof. Write $\mu(S_t) = I(r_1, r_2, t)$.

Observe $I(1,0,t) = \mu(\{y_1 \mid |y_1| \le t\}) = 2t$

& $I(0,1,t) = \mu(\{z \mid 2|z| \le t\}) = \frac{\pi t^2}{4}$

Further, for any real k, $I(r_1, r_2, kt) = k^n I(r_1, r_2, t)$, since $S_{kt} = kS_t$. $(n = r_1 + 2r_2)$.

We use induction on r_1, r_2. We have

$$I(r_1+1, r_2, t) = \int_{y=-t}^{t} I(r_1, r_2, t-|y|)\, dy$$

$$= 2\int_{y=0}^{t} I(r_1, r_2, y)\, dy$$

$$= 2\int_{y=0}^{t} I\left(r_1, r_2, t\cdot\frac{y}{t}\right) dy = 2\int_{y=0}^{t} I(r_1, r_2, y)\cdot \frac{y^n}{t^n}\, dy.$$

$$= 2\left[\frac{y^{n+1}}{n+1}\right]_0^t \cdot \frac{I(r_1, r_2, t)}{t^n} = \frac{2t}{n+1} I(r_1, r_2, t).$$

Also, $I(r_1, r_2+1, t) = \int_{\theta=0}^{2\pi}\int_{\rho=0}^{t/2} I(r_1, r_2, t-2\rho)\, \frac{\partial(x,y)}{\partial(\rho,\theta)}\, d\rho\, d\theta.$ $(\rho = |y_{r_1+r_2+1}|)$.

$$\left[z = \rho e^{i\theta},\ 2\rho \le t\right] = \int_{\theta=0}^{2\pi}\int_{\rho=0}^{t/2} I(r_1, r_2, t-2\rho)\, \rho\, d\rho\, d\theta.$$

$$= 2\pi \int_{\rho=0}^{t/2} I(r_1, r_2, \rho')\, \frac{t-\rho'}{2}\cdot\left(-\frac{1}{2}\right) d\rho' \qquad (\rho' = t-2\rho)$$

$$= -\frac{\pi}{2}\int_{\rho=t}^{0} I(r_1, r_2, 1)\, \rho^n (t-\rho)\, d\rho.$$

$$= \frac{\pi}{2} I(r_1, r_2, 1)\left(\frac{t^{n+2}}{n+1} - \frac{t^{n+2}}{n+2}\right)$$

$$= \frac{\pi t^2}{2(n+1)(n+2)} I(r_1, r_2, t).$$

$$\therefore\ I(1, 1, t) = \frac{\pi t^2}{2(2\cdot 3)} I(1, 0, t) = \frac{\pi t^3}{6}.$$

& in general $I(r_1, r_2, t) = \left(\frac{\pi}{2}\right)^{r_2}\cdot\frac{(2t)^{r_1}}{n!}$ $\left(\begin{array}{l}\text{if } n \text{ of } r_1 \text{ red},\\ n(n-1) \text{ of } r_2 \text{ red}.\end{array}\right)$ □.

Theorem 10 (Hermite). There are only finitely many fields of given discriminant d.

Pf. By cor 4", for fixed d, n is bounded. Hence we may fix n. Let $B = \{(y_1, \dots, y_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |y_1| < 2^n \left(\frac{\pi}{2}\right)^{-r_2} \sqrt{d}, |y_i| \le \frac{1}{2} \text{ for } i \neq 1\}$ $(\text{if } r_1 > 0)$

$= \{(y_1, \dots, y_{r_1+r_2}) \mid |\operatorname{Im} y_1| \le 2^n \frac{1}{\pi} \left(\frac{\pi}{2}\right)^{r_2} \sqrt{d} \text{ & } |\operatorname{Re} y_1| \le \frac{1}{4}\}$ if $r_1 = 0$.

Then B is a compact convex symmetric subset of $\mathbb{R}^n$ of volume $2^n 2^{-r_2} \sqrt{d}$. By Minkowski, $\exists\, x \in A$ such that $\sigma(x) \in B$, because $\mu(\mathbb{R}^n / \mathrm{im}\, \sigma(A)) = 2^{-r_2}\sqrt{d}$ by Cor 8!

We show that x is primitive over $\mathbb{Q}$ — i.e. that $K = \mathbb{Q}(x)$.

If $r_1 > 0$, $|\sigma_i(x)| \le \frac{1}{2}$ for $i \neq 1$. Since $|N(x)| \in \mathbb{Z}$, and $N(x) = \sigma_1(x) \cdots \sigma_n(x)$, it follows that $|\sigma_1(x)| \ge 1$. Hence $\sigma_i(x) \neq \sigma_1(x)$ $\forall\, i \ge 1$ & hence x is primitive. If $r_1 = 0$, we similarly have $|y_1| \ge 1$.

Thus K has an integer generator $x / \mathbb{Q}$, such that $\sigma(x) \in B$. Hence for fixed d, the absolute values of the conjugates of x are bounded. Hence the coeffs of the min poly of x (which are elementary symmetric functions in the conjugates of x) are bounded rational integers. Hence there are only finitely many of them.

□

If E_i = i^{th} elem symmetric function, then

$|E_i(\sigma_1(x), \dots, \sigma_n(x))| \le e^{i\beta} \cdot \binom{n}{i}$; & the E_i are the coeffs of the min poly of x (over $\mathbb{Q}$).

§7 Units in an algebraic number field.

Lemma 1. x is a unit in the ring A of integers in the alg number field $K \iff N(x) = \pm 1$.

Proof. If x is a unit $\exists\, x^{-1} \in A$ & $x x^{-1} = 1 \Rightarrow N(x)\,N(x^{-1}) = 1$, whence $N(x) = \pm 1$. Conversely if $N(x) = \pm 1$ then $N(Ax) = N(x) = 1$, whence $Ax = A$. So x is invertible. □

[Alt: if x has min poly $m(t) = t^n + a_1 t^{n-1} + \cdots + a_n$, then $N(x) = \pm a_n$, and x^{-1} satisfies $a_n t^n + a_{n-1} t^{n-1} + \cdots + 1 = 0$.]

Denote by A^* the multiplicative group of units in A.

Lemma 2. A^* is a finitely generated abelian group.

Pf. Since we are ~~only~~ interested in multiplicative structure, we take logs in the image of σ:

Define $L : K^\times \longrightarrow \mathbb{R}^{r_1+r_2}$ by

$$L(x) = \left(\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1+r_2}(x)|\right).$$

Then since $\sigma_i(xy) = \sigma_i(x)\sigma_i(y)$, L is a homom of abelian groups.

Let $B \subset \mathbb{R}^{r_1+r_2}$ be a compact subset* with diameter β. [So $|b_1 - b_2| \le \beta \;\forall\; b_1, b_2 \in B$]

If $x \in A$ and $L(x) \in B$, then $|\sigma_i(x)| < \alpha = e^\beta \;\forall i$.

Hence the number of possible min polys for x is finite & hence there are only finitely many $x \in A$ with $\sigma(x) \in B$.

In particular $\{x \in A \mid L(x) = 0\} = \ker L|_{A^*} = G$, a finite group. G therefore consists of roots of unity & is therefore cyclic.

Moreover the above argument shows that $L(A^*)$ is a discrete subgroup of $\mathbb{R}^{r_1+r_2}$ & is therefore isomorphic to $\mathbb{Z}^s$ $s \le r_1 + r_2$.

$A^* \cong G \times \mathbb{Z}^s$ is finitely generated. □

* The coeffts of the min poly are symmetric functions in the $\sigma_i(x)$ & hence are bounded.

Theorem 3. (Dirichlet's unit theorem)

Let K be an algebraic number field of degree n, r_1, r_2 as usual, $r := r_1 + r_2 - 1$. Then $A^* \cong G \times \mathbb{Z}^r$ where G is the (finite) group of roots of unity in K.

Proof. By Lemma 2, $A^* \cong G \times \mathbb{Z}^s$ where $\mathbb{Z}^s = L(A^*) \subset \mathbb{R}^{r_1+r_2}$. But any unit in A (i.e. $u \in A^*$) satisfies $|N(u)| = 1$, i.e. $N(u) = \prod_{i=1}^{r_1} |\sigma_i(u)| \prod_{r_1+1}^{r_1+r_2} |\sigma_j(u)|^2 = 1$

i.e. $L(u) \subseteq$ hyperplane $W: \sum_1^{r_1} y_i + 2\sum_{r_1+1}^{r_1+r_2} y_j = 0$ in $\mathbb{R}^{r_1+r_2}$.

Hence $L(A^*)$ is actually a discrete subgroup of $\mathbb{R}^{r_1+r_2-1}$ & so $s \le r_1 + r_2 - 1$.

To prove that $s = r_1 + r_2 - 1$, we show that for any non-zero linear form f on W, $\exists$ a unit $u \in A^*$ s.t. $f(L(u)) \neq 0$.

For the latter, observe that any linear form on W may be written $f = c_1 y_1 + \cdots + c_r y_r$, as y_{r+1} may be expressed in terms of $y_1, \ldots, y_r$ on W.

Now given an $(r+1)$-tuple $(\lambda_1, \ldots, \lambda_{r+1}) \in \mathbb{R}^{r_1+r_2}$ such that $\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j = t$ (fixed), λ_{r+1} depends on $(\lambda_1, \ldots, \lambda_r) = \lambda$

Define $S_\lambda = \{ y_1, \ldots, y_{r_1+r_2} \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |y_i| \le \lambda_i \ \forall i \}$.

S_λ is a compact, convex, symmetric subset, & $\mu(S_\lambda) = \prod_{i=1}^{r_1} 2\lambda_i \prod_{r_1+1}^{r_1+r_2} \pi \lambda_i^2$

i.e. $\mu(S_\lambda) = 2^{r_1} \pi^{r_2} t$.

Now choose t such that $2^{r_1} \pi^{r_2} t = 2^n \mu(\mathbb{R}^n / \Gamma(A))$

$= 2^n / 2^{-r_2} \sqrt{|d|}$

i.e. $t = 2^{n-r_1-r_2} \pi^{-r_2} \sqrt{|d|} = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d|}$.

Then by Minkowski, $\exists\, x_\lambda \in A$ s.t. $\sigma(x_\lambda) \in S_\lambda$, i.e. with that $|\sigma_i(x_\lambda)| \le \lambda_i \ \forall i$.

But then $|N(x_\lambda)| \le \prod_{i\le r_1} \lambda_i \prod_{r_1+1\le i\le r_1+r_2} |\lambda_i|^2 = t$,

and further, $|\sigma_i(x_\lambda)| = |N(x_\lambda)| \prod_{j\neq i} |\sigma_j^{-1}(x_\lambda)|$ (TBC).

$$\ge \lambda_i \prod_{j=1}^{r_1} \lambda_j^{-1} \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^{-2} \quad (\text{since } |N(x_\lambda)| \ge 1)$$

$$= \lambda_i\, t^{-1}$$

$\therefore \log\lambda_i \ge \log|\sigma_i(x_\lambda)| \ge \log\lambda_i - \log t$, i.e. $\log t \ge \log\lambda_i - \log|\sigma_i(x_\lambda)|$.

Multiplying by $\log|c_i|$ and adding over $i=1,\dots,r$ we see that

$$\sum_{i=1}^{r} |c_i| \log(t) \ge \left| \sum_{i=1}^{r} |c_i| \log\lambda_i - \sum_{i}^{r} |c_i| \log|\sigma_i(x_\lambda)| \right| \ge 0.$$

Hence for any $\beta > \sum_{i=1}^{r} |c_i| \log t$, $\beta > \left|\sum_i^r |c_i| \log\lambda_i - \sum_i^r |c_i| \log|\sigma_i(x)|\right|$

i.e. $\beta > \left|\sum_i |c_i| \log\lambda_i - f(L(x_\lambda))\right|$ — in this

inequality, $\lambda_1,\dots,\lambda_r$ are arbitrary positive reals (λ_{r+1} depends on them).

Now for each integer $h>0$ let $\lambda_1(h),\dots,\lambda_r(h) > 0$ be such that $\sum |c_i| |\log(\lambda_i(h))| = 2\beta h$; then writing

$$\lambda(h) = (\lambda_1(h),\dots,\lambda_r(h)), \text{ and } x_h = x_{\lambda(h)},$$

we have $\beta > |2\beta h - f(L(x_{\lambda(h)}))|$.

Hence the values of $f(L(x_h))$ are distinct for $h=1,2,3,\dots$

But $|N(Ax_h)| = |N(x_h)| \le t$. Hence there are only finitely many distinct ideals Ax_h, & so for some $h\neq k$ $Ax_h = Ax_k$, i.e. $\exists\, u \in A^*$ s.t. $x_h = x_k u$. But then $f(L(u)) = f(L(x_h)) - f(L(x_k)) \neq 0$. $\square$.

Cor 3' ∃ units $u_1, \dots, u_r$ $(r = r_1 + r_2 - 1)$ called fundamental units s.t. each unit has a unique expression

$$u = \zeta u_1^{n_1} \cdots u_r^{n_r}, \quad n_i \in \mathbb{Z}, \ \zeta \text{ a root of unity in } K.$$

Example Units in quadratic fields.

Case 1. $K = \mathbb{Q}(\sqrt{-d})$ d square free, $d > 0$. (Imaginary quadratic fields)

If $-d \equiv -1, -2 \pmod 4$ i.e. $d \equiv 1$ or $2 \bmod 4$ then the integers in K are $\{x \mid x = n + m\sqrt{-d}, \ n, m \in \mathbb{Z}\}$.

Thus $N(x) = n^2 + dm^2 = \pm 1 \iff n = \pm 1$, if $d > 1$.

Hence if $d > 1$, the only integers are ± 1

if $d = 1$, $n^2 + m^2 = 1 \iff (n, m) = (\pm 1, 0)$ or $(0, \pm 1)$.

Hence if $d = 1$, the integers are $\pm 1, \pm i$.

∴ if $d > 1$, the group U of units $\cong \mathbb{Z}/2\mathbb{Z}$.

if $d = 1$, " " " $\mathbb{Z}/4\mathbb{Z}$.

If $-d \equiv 1 \pmod 4$, i.e. $d \equiv -1 \pmod 4$ the integers are

$$\{x \mid x = \tfrac{1}{2}(n + m\sqrt{-d}), \text{ where } n, m \in \mathbb{Z}, \ m \equiv n \pmod 2\}.$$

Thus $N(x) = \frac{1}{4}(n^2 + dm^2) = 1 \iff n^2 + dm^2 = 4$.

If $d > 3$, then $d \geq 7$, so $m = 0$ and $n = \pm 2$. So $x = \pm 1$.

If $d = 3$, then we have the above solution, but in addition,

$n = \pm 1$ $m = \pm 1$.

So we have integers $\pm 1, \pm \left(\frac{1 \pm \sqrt{-3}}{2}\right)$. These are all the 6th roots of unity. So $U = A^* \cong \mathbb{Z}/6\mathbb{Z}$.

[NB: $\left(\frac{1+\sqrt{-3}}{2}\right)^2 = \frac{1}{4}(-2 + 2\sqrt{-3}) = \frac{-1+\sqrt{-3}}{2}$, $\left(\frac{1+\sqrt{-3}}{2}\right)^3 = \frac{-4}{4} = -1$].

Summary. If $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$, then $A^* \cong \mathbb{Z}/2\mathbb{Z}$, except if

$d = 1$: $A^* \cong \mathbb{Z}/4\mathbb{Z}$. $= \mu_4 \subset \mathbb{C}^*$

$d = 3$: $A^* \cong \mathbb{Z}/6\mathbb{Z}$. $= \mu_6 \subset \mathbb{C}^*$

Case 2. Real quadratic fields

Take $K = \mathbb{Q}(\sqrt{d})$ where $d > 0$ is square free. Here $r_1 = 2$, $r_2 = 0$, so by Thm 3, $A^* \cong G \times \mathbb{Z}$, where G is the (finite) group of roots of unity in K^*.

If $d \equiv 2$ or $3 \bmod 4$ then any integer $x = n + m\sqrt{d}$, $m, n \in \mathbb{Z}$. So $N(x) = n^2 - dm^2$. Since $K \subset \mathbb{R}$, we may speak of ≥ 0 for the elts of K^*, & the 4 elts x, x^{-1}, $-x$, $-x^{-1}$ are the 4 elts $\pm(n \pm m\sqrt{d})$, where $x \in A^*$. Units all have norm 1, & note if $m \neq 0$, precisely one $> \pm 1$. The largest $\pm$ in $n + m\sqrt{d}$ $(n, m \geq 0)$. & so the units > 1 are those of the form $n + m\sqrt{d}$, $m, n \neq \in \mathbb{Z}_{>0}$.

Units are solutions of the Pell-Fermat equation

$$n^2 - dm^2 = \pm 1.$$

Dirichlet $\Rightarrow$: the set of solutions is obtained as follows:

$\exists$ fundamental solution (n_1, m_1) s.t. each solution (n_k, m_k) is given by:

$$(n_k + m_k\sqrt{d}) = (n_1 + m_1\sqrt{d})^k \quad (k > 0).$$

So $(n_{k+1} + m_{k+1}\sqrt{d}) = (n_k + m_k\sqrt{d})(n_1 + m_1\sqrt{d})$

$$= n_k n_1 + d m_k m_1 + (n_k m_1 + m_k n_1)\sqrt{d}.$$

$\therefore m_{k+1} > m_k$. Hence to find m_1, look at $m^2 d$ $(m = 1, 2, \dots)$ & find the first m s.t. $m^2 d$ differs from a square by ± 1.

The solutions of $n^2 - dm^2 = +1$ are the even powers of the fundamental solution (if $N(\text{fund}) = -1$) or all powers if $N(\text{fund}) = 1$.

We have shown: ✓

Prop If $d \equiv 2$ or $3 \bmod 4$, $A^* = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} = \{\pm 1\} \times \mathbb{Z}$, where $\mathbb{Z}$ = set of positive units.

Example. $d = 3$; look at $d, 4d, 9d, \dots = 3, 12, 27, \dots$; which is first to differ from a square by ± 1? $2^2 - 3 = 1$ so $2 + \sqrt{3}$ is a unit & generates A^* mod $\mathbb{Z}/2\mathbb{Z}$; norm $= 1$. So $A^* = \{\pm(2 + \sqrt{3})^k \mid k = 0, \pm 1, \pm 2, \dots\}$

$d=7$: $8+3\sqrt{7}$ is a fund unit.

If $d \equiv 1 \pmod 4$, the integers are of the form $x = \frac{1}{2}(n + m\sqrt{d})$
$m, n \in \mathbb{Z}$, $n \equiv m \pmod 2$. So $N(x) = \frac{1}{4}(n^2 - m^2 d) = \pm 1 \iff$
$n^2 - dm^2 = \pm 4$.

As above, if $\frac{1}{2}(n_1 + m_1\sqrt{d})$ is the fundamental unit, the units are of the form $\frac{1}{2}(n_k + m_k\sqrt{d})$, where
$$\frac{1}{2}(n_k + m_k\sqrt{d}) = \frac{1}{2^k}(a_1 + m_1\sqrt{d})^k$$

[NB as before, the 4 units $\pm\frac{1}{2}(n \pm m\sqrt{d})$ are the 4 units $\pm x^{\pm 1}$, $\pm$ the rest and just one of these > 1].

Examples (i) $d=5$. fund unit $\frac{1+\sqrt{5}}{2}$.

(ii) $d=13$ fund unit $\frac{3+\sqrt{13}}{2}$

(iii) $d = 17$. Fund unit $4+\sqrt{17}$.

Exercise Let $B(r)$ be the r-ball defined by
$B(r) = \{ x \in \mathbb{R}^n \mid x.x < r^2 \}$. ($x.x = \sum x_i^2$ if $x = (x_1, \dots, x_n)$).

Show that $\mathrm{Vol}(B_r) = \omega_n r^n$ where

$$\omega_n = \int_0^{2\pi}\int_0^1 \omega_{n-2}\left(\sqrt{1-r^2}\right)^{n-2} r\,dr\,d\theta = 2\pi\,\omega_{n-2}/n.$$

Deduce that $\omega_n = \begin{cases} \frac{\pi^m}{m!} & \text{if } n = 2m. \\ \frac{2^{m+1}\pi^m}{1\cdot 3\cdots(n-2)\cdot n} & \text{if } n = 2m+1. \end{cases}$

$n = 4 = 2\times 2$. $\omega_4 = \frac{\pi^2}{2}$

§8 Sums of two and four squares.

We make a small interlude to prove two ancient theorem in a beautiful way, using Minkowski's theorem.

Thm 1. (Fermat, 17th; Euler 18th) If p is a prime number of the form $4k+1$, the equation $a^2+b^2=p$ has a solution with $a, b \in \mathbb{Z}$.

Proof. The congruence $u^2 \equiv -1 \pmod p$ has a solution with $u \in \mathbb{Z} \iff p \equiv 1 \bmod 4$ (i.e. $4 \mid p-1$).
So choose such a u and define $L \subseteq \mathbb{Z} \oplus \mathbb{Z} \subseteq \mathbb{R}^2$ as the subgroup $L = \{(a,b) \in \mathbb{Z}\oplus\mathbb{Z} \mid b \equiv ua \bmod p\}$.
$= \ker\left(\varphi : \mathbb{Z}\oplus\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}\right)$,
where $\varphi(a,b) := b - ua \pmod p$.
Then φ is surjective & so $\mathbb{Z}\oplus\mathbb{Z}/L \cong \mathbb{Z}/p\mathbb{Z}$ &
hence $\mu(L) = |\mathbb{Z}\oplus\mathbb{Z}/L| = p$.

Hence by Minkowski's theorem, taking $D = B(r)$, where $\mu(B(r)) = \pi r^2$ satisfies $\pi r^2 = 2^2 p$, i.e. $r = \sqrt{\frac{4p}{\pi}}$, we conclude $\exists$ a non-zero point $x \in L \cap B(r)$, i.e. s.t. $x \cdot x \le \frac{4p}{\pi}$

$\therefore$ if $x = (a,b)$, $0 < a^2+b^2 \le \frac{4p}{\pi} < 2p$.

But mod p, $a^2+b^2 \equiv a^2+u^2a^2 = 0$; so $a^2+b^2 \equiv 0 \bmod p$,
& hence $= p$. $\square$

Cor 1 The subset of $\mathbb{Q}^*$ consisting of non-zero elts expressible as a sum of 2 squares is a f.a.g. with generators $2, 3^2, 5, 7^2, 11^2, 13, \ldots$

Pf. Note that $n \in \mathbb{Z}$, is a sum of 2 squares $\Leftrightarrow n = z\bar{z}$ for $z = a+ib \in \mathbb{Z} \oplus i\mathbb{Z}$. But $|z_1 z_2|^2 = |z_1|^2 |z_2|^2$, so n, m are sums of 2 squares $\Rightarrow nm$ also is. Further, $|z|^{-2} = |z^{-1}|^2$; if $z \in \mathbb{Q}^* \oplus i\mathbb{Q}^*$, then $z^{-1} = \frac{\bar{z}}{|z|^2} \in \mathbb{Q} \oplus i\mathbb{Q}$.
$(z\bar{z} = |z|^2 \Rightarrow z^{-1} = \frac{\bar{z}}{|z|^2})$.

$\therefore$ (eg. $5 = 1^2 + 2^2 \Rightarrow \frac{1}{5} = |(1+2i)^{-1}| = \left|\frac{1-2i}{5}\right|$
$= \left(\frac{1}{5}\right)^2 + \left(\frac{2}{5}\right)^2$)

Hence the result. □

Theorem 2. (Bachet de Méziriac 17th cent. Pf by Lagrange, 18th).
Every positive integer is the sum of 4 squares.

Pf. Fix an odd prime p. The congruence $u^2 + v^2 + 1 \equiv 0 \pmod{p}$ has a solution in integers, for $|\{-v^2 - 1 \mid v \in \mathbb{F}_p\}| = \frac{p+1}{2}$ $(= \frac{p-1}{2} + 1)$
and $|\{u^2\}| = \frac{p+1}{2}$

Hence these 2 sets intersect

Fix $u, v \in \mathbb{Z}$ satisfying the congruence, and define

$$L := \{(a,b,c,d) \in \mathbb{Z}^4 \mid c \equiv ua + vb \pmod{p}, \quad d \equiv ub - va \pmod{p}\}.$$

Then $L = \ker \varphi$, where $\varphi : \mathbb{Z}^4 \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is defined by

$(a,b,c,d) \longmapsto (c - ua - vb, \; d - ub + va) \pmod{p}$. — surjective.

Hence $\mu(L) = |\mathbb{Z}^4 / L| = p^2$.

Taking S in Minkowski to be $B(r)$ st $\mu(B(r)) = \frac{\pi^2}{2} r^4$

satisfies $2^4 \cdot p^2 = \frac{\pi^2}{2} r^4$

i.e. $r^2 = \frac{2^2 \sqrt{2}\, p}{\pi}$ i.e. $r = 2 \cdot 2^{\frac{1}{2}} \sqrt{\frac{p}{\pi}}$

Now $\exists\, x \in L$ with $x \cdot x \leq r^2$, i.e. $\leq \frac{4\sqrt{2}}{\pi} p < 2p$,

But again $x \cdot x = a^2 + b^2 + u^2 a^2 + v^2 b^2 + a^2 b^2 + v^2 a^2$

$= (a^2+b^2)(1 + a^2 + v^2)$

$\equiv 0 \pmod{p}$.

$\therefore x \cdot x = p$ as above.

But recall that if $\mathbb{H} = \{a + ib + jc + kd\}$ is the set of quaternions,

$|x||y| = |xy|$.

Moreover $n = N(x)$ for some $x \in H_{\mathbb{Z}} \Leftrightarrow n$ is the sum of 4 squares. Hence the set of such integers is multiplicatively closed, & since it contains all primes, it $= \mathbb{Z}_{\geq 1}$. ☐

over.

§9 Factorisation of Ideals in Extension Fields.

The basic question illustrated by the fact that if $p \in \mathbb{Z}$ is prime, then pA is not necessarily a prime ideal.

Eg. pA is a prime ideal $\Leftrightarrow$ A/pA is a field (recall: prime $\Leftrightarrow$ maximal). Ex: $A = \mathbb{Z}[\sqrt{-5}]$. $|A/2A| = 4 = N(2)$. $A/2A$ is an extension of $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ by $x = \sqrt{-5}$. But $x^2 = -1$ so $(1+x)^2 = 0$; hence $A/2A$ is not a field as $A/2A = \frac{\mathbb{F}_2[x]}{(1+x)^2}$; to get a field, need $\frac{\mathbb{F}_2[x]}{(1+x+x^2)}$.

But: pA is a product of prime ideals.

Definition Let A be an integral domain with quot field K, S a mult-closed subset of A not containing 0, but st. $1 \in S$. The localisation of A at $A-S$ is $A_S = S^{-1}A := \{\frac{a}{s} \in K \mid a \in A, s \in S\}$.

Ex. If $\mathfrak{p} \subset A$ is a prime ideal, $S = A - \mathfrak{p}$, then $A_{\mathfrak{p}}$ = localisation at $\mathfrak{p}$. If $S = A \setminus \{0\}$, get $A_S = K$.

Recall (from Commutative Algebra):

Proposition 1. Let $A \subset K$, S be as above, $A' = S^{-1}A$. Then
(i) For each ideal $\mathfrak{b}' \trianglelefteq A'$ we have $(\mathfrak{b}' \cap A)A' = \mathfrak{b}'$. Hence $\mathfrak{b} \mapsto \mathfrak{b}' \cap A$ is a strictly monotonic injection of the set of ideals of A' into the ideals of A.
(ii) The map $\mathfrak{p}' \mapsto \mathfrak{p}' \cap A$ is a lattice (poset) isomorphism from the set of prime ideals $\mathfrak{p}'$ of A' to the prime ideals $\mathfrak{p} \trianglelefteq A$, such that $\mathfrak{p} \cap S = \phi$.
The inverse of this map is $\mathfrak{p} \mapsto A'\mathfrak{p}$.

Proof - (i) We have $(\mathfrak{P}' \cap A)A' \subseteq \mathfrak{P}A' = \mathfrak{P}$. To prove the converse take $x = \frac{a}{s} \in \mathfrak{P}'$; then $a \in \mathfrak{P} \cap A$ since $a = x \cdot s$, and since $\frac{1}{s} \in A'$, $\frac{a}{s} = a \cdot \frac{1}{s} \in (\mathfrak{P} \cap A)A'$.

Clearly the map $\mathfrak{P} \mapsto \mathfrak{P} \cap A$ is inclusion-preserving, and is injective by what we have proved. [Of course $\mathfrak{P} \cap A$ is an ideal of A].

(ii) If $\mathfrak{P}'$ is a prime ideal of A', then evidently $\mathfrak{P} = A \cap \mathfrak{P}'$ is a prime ideal of A [if $ab \in \mathfrak{P}$, then $ab \in \mathfrak{P}'$, so $a \in \mathfrak{P}'$ or $b \in \mathfrak{P}'$]. Further, if $s \in \mathfrak{P} \cap S$, then $s \in \mathfrak{P}'$, so $\frac{1}{s} \cdot s = 1 \in \mathfrak{P}'$, which is impossible. Hence $\mathfrak{P} \cap S = \phi$. Hence $\mathfrak{P}' \mapsto \mathfrak{P}' \cap A$ takes prime ideals of A' to prime ideals $\mathfrak{P}$ of A s.t. $\mathfrak{P} \cap S = \phi$. (s.t. $\mathfrak{P} \cap S = \phi$)

Conversely if $\mathfrak{P}$ is a prime ideal of A, we need to show that $A'\mathfrak{P}$ is a prime ideal of A' & that $\mathfrak{P} = A'\mathfrak{P} \cap A$. For this, write $\mathfrak{P}' = A'\mathfrak{P}$. Now $\mathfrak{P}' = \left\{ \frac{p}{s} \mid p \in \mathfrak{P}, s \in S \right\}$, for if $x \in \mathfrak{P}'$, $x = \sum \frac{a_i p_i}{s_i} = \frac{\sum \pi s_j a_i p_i}{\pi s_i} = \frac{p}{s}$

(Note: $\frac{p_1}{s_1} + \frac{p_2}{s_2} = \frac{p_1 s_2 + p_2 s_1}{s_1 s_2} = \frac{p_3}{s_3}$)

Now if $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{p}{s} \in A'\mathfrak{P}$, then $s a_1 a_2 = p s_1 s_2$

$\therefore s a_1 a_2 \in \mathfrak{P}$. But $s \notin \mathfrak{P}$ so $a_1 a_2 \in \mathfrak{P}$ Hence $a_1 \in \mathfrak{P}$ or $a_2 \in \mathfrak{P}$.

$\therefore \frac{a_1}{s_1} \in \mathfrak{P}'$ or $\frac{a_2}{s_2} \in \mathfrak{P}'$. Hence $\mathfrak{P}' = A'\mathfrak{P}$ is a prime ideal.

Finally, $A'\mathfrak{P} \cap A \supseteq \mathfrak{P}$, and if $p \in A$, then $p = sa$ and again $s \notin \mathfrak{P} \Rightarrow a \in \mathfrak{P}$. So $A'\mathfrak{P} \cap A = \mathfrak{P}$. D.

Cor 1 If A is noetherian, so is $S^{-1}A = A'$.

Pf. A chain of ideals in A' has chain in A. Since the latter terminates so does the former. D.

Integral closure and localisation.

Lemma 2. Let $A \subset S$ be as in Prop 1, and let R be an integral domain containing A. Let B be the integral closure of A in R, $B' =$ integral closure of $A' = A_S$ in R_S. Then $B' = B_S = S^{-1}B$.

Proof. If $\frac{r}{s} \in B'$, there is an equation of the form

$$\left(\frac{r}{s}\right)^n + \frac{a_{n-1}}{s_{n-1}}\left(\frac{r}{s}\right)^{n-1} + \cdots + \frac{a_0}{s_0} = 0.$$

Hence $\frac{r}{s}, s_0 \cdots s_{n-1}$ is integral over A & hence $\in B$. (mult by $(s_0 \cdots s_{n-1})^n$.).

$\therefore \frac{r}{s} \in S^{-1}B$. So $B' \subseteq S^{-1}B$.

Conversely if $b \in B$ $s \in S$ then b satisfies

$b^n + a_1 b^{n-1} + \cdots + a_n = 0$ $(a_i \in A)$, & so

$\left(\frac{b}{s}\right)^n + \frac{a_1}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^{n-1}} = 0$, so $\frac{b}{s} \in B'$. □

Cor 2'. If A is integrally closed, so is every localisation of A.

Pf. Take $R = K$ in the Lemma. Then $B = A$ & so $B' = S^{-1}A =$ int closure of $S^{-1}A$. □

Cor 2'' If A is a Dedekind domain, so is every localisation $S^{-1}A$.

Pf. Recall: A is DD iff (a) A is int closed &
(b) A is noetherian.
(c) Every prime ideal is maximal.

We've seen that (a), (b) hold for $S^{-1}A$ $\forall S$ in the last 2 results & for (c), if by Prop 1 (ii), if $\mathfrak{P}'$ is a prime ideal of A', then $\mathfrak{P}' \subseteq \mathfrak{m}'$ $\Rightarrow$ $\mathfrak{P}' \cap A \subseteq \mathfrak{m} \cap A$; but equality in the latter (A is DD) $\Rightarrow \mathfrak{P}' = \mathfrak{m}'$. □

Our purpose is to study ramification of primes. For this we need 2 more general results.

Proposition 3. Let A be a Dedekind domain, $\mathfrak{p} \neq 0$ a prime ideal of A and $S = A \setminus \mathfrak{p}$. Then $S^{-1}A$ is a PID; in fact $\exists$ a unique maximal ideal $\mathfrak{m} = \langle \mathfrak{P} \rangle$ in A_S, such that all ideals are of the form $\mathfrak{m}^r = \langle \mathfrak{P}^r \rangle$ $(r = 0, 1, 2, \cdots)$. [This says: $S^{-1}A$ is a local ring].

Pf. Let $A' = A_S = \{\frac{a}{s} \mid a \in A, s \in S\}$. We've seen that there's a bijection between the prime ideals of A' and those of A such that $\mathfrak{q} \cap S = \phi$. But any such prime ideal $\subset \mathfrak{p} = A \setminus S$ since $S^{-1}\mathfrak{p} \neq 0$ is the unique ~~maximal~~ prime ideal of A'.

Since $S^{-1}A$ is a Dedekind domain all ideals are powers of $\mathfrak{m}$ (recall: any ideal is a product of prime ideals)

Now take any element $p \in \mathfrak{m}$ s.t. $p \notin \mathfrak{m}^2$. Then $\langle p \rangle_{A'} = \mathfrak{m}$, (since $\subset \mathfrak{m}$ but $\not\subset \mathfrak{m}^2$). Hence all ideals are of the form $\langle p^r \rangle_{A'}$. □.

Finally, to calculate quotients, we have

Lemma 4. Let A be an integral domain, S as above, $\mathfrak{m}$ a max'l ideal of A with $\mathfrak{m} \cap S = \phi$. Then
$$A'/\mathfrak{m}A' \cong A/\mathfrak{m}.$$

Proof. The homomorphism $A \to S^{-1}A \to S^{-1}A/\mathfrak{m}S^{-1}A$ has kernel precisely $\mathfrak{m}$, since the kernel is a max'l ideal. To see that the map is surjective, take $\frac{a}{s} \in S^{-1}A$. Since $s \notin \mathfrak{m}$, $\exists\ t \in A$ s.t. $st \equiv 1 \bmod \mathfrak{m}$ i.e. $t \equiv \frac{1}{s} \bmod A'\mathfrak{m}$.
$\therefore \frac{a}{s}$ is the image of at under the above map.
$(at \equiv \frac{a}{s} \bmod A'\mathfrak{m})$ □.

Now apply the above generalities to alg number fields:

A Dedekind domain
K its quot field.
L finite, degree n extension of K.
B int closure of A in L.

We assume $\mathbb{C} \supset L \supset K \supset A$

B

Let $\mathfrak{P}$ be a non-zero prime of A. Then $B\mathfrak{P}$ is an ideal of B

$\ast$ & we have $\boxed{B\mathfrak{P} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}}$ where $\mathfrak{p}_i$ are prime ideals of B,

We now proceed to study this decomposition of $B\mathfrak{P}$.

Lemma 5: The $\mathfrak{p}_i$ above are precisely the prime ideals $\mathfrak{p}$ of B which satisfy $\mathfrak{p} \cap A = \mathfrak{P}$

Pf. (Trivial observation). We have $\mathfrak{p} \supset B\mathfrak{P} \Leftrightarrow \mathfrak{p} \supset \mathfrak{P}$
$\Leftrightarrow \mathfrak{p} \cap A \supset \mathfrak{P}$ (easy) $\square$

It follows that for any such $\mathfrak{p}_i$:

$$\frac{A}{\mathfrak{P}} = \frac{A}{\mathfrak{p} \cap A} = \frac{A+\mathfrak{p}}{\mathfrak{p}} \leq \frac{B}{\mathfrak{p}} \quad \text{(both finite fields)}.$$

So the field $\frac{A}{\mathfrak{P}}$ is naturally a subfield of $\frac{B}{\mathfrak{p}}$.

In particular, $\frac{B}{\mathfrak{p}}$ is a finite dimensional vector space over $\frac{A}{\mathfrak{P}}$.

Defn. The residual degree of $\mathfrak{p}_i$ over A is f_i, where

$$f_i = \dim_{A/\mathfrak{P}} (B/\mathfrak{p}_i)$$

The index of ramification of $\mathfrak{p}_i$ over A is the power e_i occurring in the decomposition of $\mathfrak{P}$. $(= \mathfrak{p}_i \cap A)$

NB We have $B\mathfrak{p} \cap A = \mathfrak{p}$

For certainly $B\mathfrak{p} \cap A \supseteq \mathfrak{p}$, and is an ideal of A.
So $B\mathfrak{p} \cap A = \mathfrak{p}$ or $B\mathfrak{p} \cap A = A$. If $B\mathfrak{p} \supseteq A$, then $1 \in B\mathfrak{p}$, so $B\mathfrak{p} = B$. [But this is impossible since for any prime ideal $\mathfrak{P}$ of B s.t. $\mathfrak{P} \cap A = \mathfrak{p}$ (and these exist because $B\mathfrak{p}$ does have a decomposition $\prod \mathfrak{P}_i^{e_i}$), we have $\mathfrak{P} \supseteq B\mathfrak{p}$]

Proof that $B\mathfrak{p} \cap A \neq A$. Observe that $\bigcap_{i \geq 0} \mathfrak{p}^i = 0$, for if $x \in \bigcap_{i \geq 0} \mathfrak{p}^i$, then $xA \subset \mathfrak{p}^i$ $\forall i \geq 0$ & so $\mathfrak{p}^i \mid xA$ $\forall i$.

$B\mathfrak{p} \cap A = A \Rightarrow B\mathfrak{p} = B$.

[Contradicts unique factorization of ideals. But if $B\mathfrak{p} = B$, then $B = B\mathfrak{p} = B\mathfrak{p}^2 = B\mathfrak{p}^3 = (B\mathfrak{p})^i$. To show $B\mathfrak{p} \neq B$ (equivalently $1 \notin B\mathfrak{p}$) we use a determinant formula.
[If $B\mathfrak{p} \cap A = A$, then $B\mathfrak{p} = B$; so $1 \in B\mathfrak{p}$, $B\mathfrak{p} = B\mathfrak{p}^2 = \ldots$ i.e. $1 \in B$]

Theorem 5 With the above notation we have:

$$\sum_i e_i f_i = n = [B/B\mathfrak{p} : A/\mathfrak{p}] = [L : K].$$

Pf. For any ideal $\mathfrak{P}$ of B and any $\mathfrak{P}_i$ as above, we have that $\frac{B}{\mathfrak{P}_i}$ is a field, and $\frac{\mathfrak{P}}{\mathfrak{P}\mathfrak{P}_i}$ has an action of B, with $\mathfrak{P}_i$ acting trivially. So $\frac{\mathfrak{P}}{\mathfrak{P}\mathfrak{P}_i}$ is a vector space over $\frac{B}{\mathfrak{P}_i}$.

Any subspace of $\frac{\mathfrak{P}}{\mathfrak{P}\mathfrak{P}_i}$ corresponds to an ideal $\mathfrak{A}$ s.t. $\mathfrak{P} \supseteq \mathfrak{A} \supseteq \mathfrak{P}\mathfrak{P}_i$ (by unique factorization).

By the maximality of $\mathfrak{P}_i$ in B, $\mathfrak{P}\mathfrak{P}_i$ is max'l in $\mathfrak{P}$. So $\dim_{\frac{B}{\mathfrak{P}_i}} \left(\frac{\mathfrak{P}}{\mathfrak{P}\mathfrak{P}_i}\right) = 1$ & so $\frac{\mathfrak{P}}{\mathfrak{P}\mathfrak{P}_i} \cong \frac{B}{\mathfrak{P}_i}$ for any $\mathfrak{P} \triangleleft B$

$\#(A/\mathfrak{p})^i$.

Now consider the sequence

$$B \supset \mathfrak{P}B \supset \mathfrak{P}^2 \supset \cdots \supset \mathfrak{P}^{e_1} \supset \mathfrak{P}^{e_1}\mathfrak{P}_2 \supset \mathfrak{P}^{e_1}\mathfrak{P}_2^2 \supset \cdots \supset \mathfrak{P}^{e_1}\mathfrak{P}_2^{e_2} \supset \cdots \supset B\mathfrak{P} = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$$

The quotients in this chain have dimension f_i over $A/\mathfrak{P}$, and since there are e_i quotients corresp to $\mathfrak{P}_i$, we have

$$\dim_{A/\mathfrak{P}} (B/B\mathfrak{P}) = \sum_{i=1}^{g} e_i f_i. \qquad \text{(e.g. if } A \text{ is a PID)}$$

On the other hand, if B is a free A-module with basis $x_1, \ldots, x_n$ then $x_1, \ldots, x_n$ is a basis of $B/B\mathfrak{P}$ over $A/\mathfrak{P}$

Hence $\sum e_i f_i = n$ in this case (e.g. if A is a PID) ∎

In general we reduce to the case where A is a PID by localizing at $S = A \setminus \mathfrak{P}$. Then A' is a PID $B' = S^{-1}B$ is the int closure of A' in L, and there is a prime ideal $\mathfrak{P}'$ of B' which satisfies $\mathfrak{P}' \cap A' = \mathfrak{P}' \iff \mathfrak{P}' = S^{-1}\mathfrak{P}$ for some prime ideal $\mathfrak{P}$ of B with $\mathfrak{P} \cap S = \emptyset$ (i.e. $\mathfrak{P} \subset \mathfrak{P}$).

Moreover $[B'/\mathfrak{P}B' : A'/A'\mathfrak{P}] = n$ by the PID case.

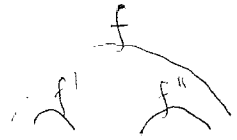
But $A'/A'\mathfrak{P} \cong A/\mathfrak{P}$ by Lemma 4.

Furthermore, $\mathfrak{P}B = \prod \mathfrak{P}_i^{e_i} \Rightarrow \mathfrak{P}B' = \prod (\mathfrak{P}_i')^{e_i}$, where

$\mathfrak{P}_i' = B'\mathfrak{P}_i$ is a prime ideal of B', and by again by Lemma 4, $B'/\mathfrak{P}_i' \cong B/\mathfrak{P}_i$. So by the argument above,

$$\dim_{A'/\mathfrak{P}'} B'/\mathfrak{P}B' = \dim_{A/\mathfrak{P}} B/B\mathfrak{P} = n = \sum e_i f_i. \qquad \square$$

Start with this: $B/\mathfrak{P}B$ is a v.s. over $A/\mathfrak{P}$, and say $\dim_{A/\mathfrak{P}} (B/\mathfrak{P}B) = n$.



Problem. Suppose $K \subset K' \subset K'' \subset \mathbb{C}$ are of number fields, $\mathfrak{P}''$ a maximal ideal of A''. Let $\mathfrak{P}' = \mathfrak{P}'' \cap K'$, $\mathfrak{p} = \mathfrak{P}'' \cap K$.

Let f = residual degree of $\mathfrak{P}''$ over K.

f' = " " " $\mathfrak{P}'$ " K.

f'' = " " " $\mathfrak{P}''$ " K'.

Similarly for ramification indices e, e', e''.

Show that $e = e'e''$ and $f = f'f''$.

Example. Cyclotomic fields.

Let p be a rational prime, z a primitive $(p^r)^{th}$ root of unity ($r \geq 1$). We investigate the field

$K = \mathbb{Q}(z)$

Consider the polynomial $m(t) = \dfrac{t^{p^r}-1}{t^{p^{r-1}}-1} = 1 + t^{p^{r-1}} + t^{2p^{r-1}} + \cdots + t^{(p-1)p^{r-1}}$

We show 1st that $m(t)$ is irred, and $[\mathbb{Q}(z) : \mathbb{Q}] = p^{r-1}(p-1)$

We then investigate Bp, where B = integers in $\mathbb{Q}(z)$.

Let $z_1, \ldots, z_n$ be the primitive $(p^r)^{th}$ roots of unity. Since $m(1) = p$ and $m(t) = \prod_{i=1}^{n} (t - z_i)$, we have $\prod_{i=1}^{n} (1 - z_i) = \pm p$

Further, $\forall i,j$ $z_i = z_j^k$, so $(1 - z_i) = (1 - z_j)$ unit.

$\therefore B(z_i - 1) = B(z_j - 1)$.

$\therefore Bp = B \prod_{i=1}^{n} (z_i - 1) = B(1 - z_1)^n$.

But $Bp = \prod \mathfrak{p}_i^{e_i}$, where $\sum e_i f_i = \deg K \leq n$.

$\therefore e_1 = n \Rightarrow f_1 = 1$, & $n = \deg K/\mathbb{Q}$, and $m(t)$ is irred.

$B(1 - z_1)$ is prime; $B / B(1 - z_1) \cong \mathbb{F}_p$.

and $B\mathfrak{p} = \left(B(1-z_1)\right)^n$.

This says that $\mathfrak{p}$ is totally ramified in K (the "worst possible" case.).

§10 Ramification. We investigate what possible values the indices e_i, f_i might take. Notation is as in §9. The main result we are aiming at is that primes generically are unramified, and the singular cases can be identified by the discriminant.

Recall the following facts about discriminants:

If B is a free A-module, A a Dedekind domain and $x_1, \dots, x_n \in B$, then $\Delta_{B/A}(x_1, \dots, x_n) = \det\left(\mathrm{Tr}(x_i x_j)\right)$.

$\Delta_{B/A}$ = ideal generated by $\Delta_{B/A}(x_1, \dots, x_n)$ when $x_1, \dots, x_n$ is an A-basis of B. This is determined up to mult by an invertible elt of A.

We are concerned with the case where A, B are rings of integers — i.e.

A is a Dedekind domain with quot fld K, an alg no. fld.

L is a finite, separable extension of K.

B = set of elements of L which are integral over A.

Defn. The discriminant $\Delta_{B/A} = \Delta_{L/K}$ is the ideal of A generated by the discriminants of all bases of L over K which are contained in B.

Remarks. 1) The discrim of any basis of L, cont in B, is an elt of A.

2) B may not be a free A-module (eg if A is not a PID), so this defn $\neq \Delta_{B/A}$. If B is a free A-module, the defns coincide.

Our main objective is:

Theorem 1. *In the notation of the above definition, the prime ideal $\mathfrak{p}$ of A is ramified in $B \iff \mathfrak{p}$ divides $\Delta_{B/A}$. In particular, there are only finitely many ramified primes.*

We prove several preliminary results.

Lemma 2. *$\mathfrak{p}$ is ramified in $B \iff B/B\mathfrak{p}$ contains non-zero nilpotent elements.*

Pf. We have $B\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$, however for $i \neq j$, we have $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = B$, for if $\mathfrak{P}$ is a prime ideal of B such that $\mathfrak{P} \supseteq \mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j}$ then $\mathfrak{P} \supseteq \mathfrak{P}_i \ni \mathfrak{P} \supseteq \mathfrak{P}_j \ni$ so $\mathfrak{P} \supseteq \mathfrak{P}_i + \mathfrak{P}_j = B$, in fact $\mathfrak{P}_i^{e_i} + \prod_{j \neq i} \mathfrak{P}_j^{e_j} = B$.

It follows that:

$$\boxed{B/B\mathfrak{p} = \prod_{i=1}^{r} B/\mathfrak{P}_i^{e_i}.} \qquad *$$

[This follows from the general fact that if $B_1, B_2 \trianglelefteq B$, $B_1 + B_2 = B$ then $\frac{B}{B_1 \cap B_2} \cong \frac{B}{B_1} \times \frac{B}{B_2}$, for $B \to \frac{B}{B_1} \times \frac{B}{B_2}$ surj by CRT, Chinese R.T. has kernel $B_1 \cap B_2$.]

$\therefore B/B\mathfrak{p}$ contains a non-zero nilp. element $\iff e_i \geq 2$ for some $i \iff \mathfrak{p}$ is ramified in B. $\square$

Remember the isom $*$.

We now relate the discriminantal condition to that of the existence of non-zero nilpotent elements.

Lemma 3: (i) Let A be an integral domain, and $B_1, \dots, B_q$ free A-modules. Then, writing $B = B_1 \times \cdots \times B_q$, $\Delta_{B/A} = \prod_{i=1}^{q} \Delta_{B_i/A}$ (product of ideals of A).

(ii) If $\mathfrak{a}$ is any ideal of A, denote by $\bar{x}$ the class of $x \in B$ modulo $B\mathfrak{a}$. If $x_1, \dots, x_n$ is a basis of B/A, then $\bar{x}_1, \dots, \bar{x}_n$ is a basis of $B/B\mathfrak{a}$ over $A/\mathfrak{a}$, and

$$\Delta(\bar{x}_1, \dots, \bar{x}_n) = \Delta(x_1, \dots, x_n).$$

Proof (i) A basis of B is obtained by juxtaposing bases of the B_i over A. Since if $x_i \in B_i$, $x_j \in B_j$, $i \neq j$ we have $x_i x_j = 0$, it follows that $\mathrm{tr}(x_i x_j) = 0$, and therefore the matrix of $\mathrm{tr}(xx')$ of this basis is block diagonal, & the result is obvious.

(ii) Any element $x \in B$ satisfies $x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0$, $a_i \in A$, so $\bar{x}^n + \sum_{i=1}^{n} \bar{a}_i \bar{x}^{n-i} = 0$. If $\sum_{i=1}^{n} \bar{a}_i \bar{x}_i = 0$, then

$\sum a_i x_i \in B\mathfrak{a}$, so $\sum a_i x_i = \sum \mu_i x_i$ with $\mu_i \in \mathfrak{a}$. Hence $a_i \in \mathfrak{a}$ $\forall i$. Hence the $\bar{x}_i$ are indep over $A/\mathfrak{a}$. If (a_{ij}) = matrix of m_x $(x \in B)$ then $(\bar{a}_{ij})$ is the matrix of $m_{\bar{x}}$. Hence $\mathrm{tr}(\bar{x}_i \bar{x}_j) = \overline{\mathrm{tr}(a_{ij})}$, and the result follows. □

Prop 4. (i) If the noetherian ring R contains no nilpotent elements ($\neq 0$), then (0) is the intersection of a finite number of prime ideals.

(ii) Let k be a perfect field, L a finite-dimensional algebra over k. Then L contains non-zero nilpotent elements $\Leftrightarrow \Delta_{L/k} = 0$.

Proof. (i) (a) Define $I \trianglelefteq R$ to be irred if $I = I_1 \cap I_2 \Rightarrow I = I_1$ or $I = I_2$. Since R is noetherian, any ideal is a *finite* intersection of irred ideals: for if $I = I_1 \cap I_1'$, $I_1 = I_2 \cap I_2'$, $I_2 = I_3 \cap I_3'$, ... we have $I_1 \subset I_2 \subset I_3 \subset \cdots$, so this process terminates.

(b) If R contains no nilpotent elements, every irred ideal is prime. Let I be irred; replacing R by R/I RTP R is an integral domain (i.e. (0) is irreducible). Suppose $xy = 0$, $x \neq 0$. Since $\operatorname{Ann}(y^n) \subseteq \operatorname{Ann}(y^{n+1})$, $\exists N$ s.t. $\operatorname{Ann} y^N = \operatorname{Ann} y^{N+1} = \operatorname{Ann} y^{N+2} = \cdots$.

Suppose $z \in (x) \cap (y^N)$. Then $z = rx = sy^N$. $\therefore zy = rxy = 0 = sy^{N+1}$. So $s \in \operatorname{Ann} y^{N+1} = \operatorname{Ann} y^N$. Hence $z = 0$. Therefore $(x) \cap (y^N) = 0$. By irreducibility, $y^N = 0$. ($(x) \neq 0$).

(b) Every irred ideal is primary: let I be irred and suppose $xy \in I$, $x \notin I$. Let $J_n = \{r \in R \mid ry^n \in I\}$. Then $J_n \subset J_{n+1}$, & since R is noeth, $J_N = J_{N+1} = \cdots$ some N. Let $z \in (x) \cap (y^N)$. Then $z = rx = sy^N$, and $zy = rxy = sy^{N+1} \in I$. So $s \in J_{N+1} = J_N$ & so $sy^N \in I$, so $(x) \cap (y^N) \subseteq I$. Hence $(x+I) \cap (y^N + I) = I$ & by irreducibility $x \notin I \neq I \Rightarrow y^N + I = I$, i.e. $y^N \in I$.

(c) If Q is primary, $\sqrt{Q} = P = \{y \mid y^r \in Q, \text{ some } r\}$ is a prime ideal.

(d) By (a), (b), $(0) = Q_1 \cap \cdots \cap Q_r$, Q_i primary. Consider $P_1 \cap \cdots \cap P_r$ where $P_i = \sqrt{Q_i}$. If $x \in J$, then $x^N \in Q_1 \cap \cdots \cap Q_r$, some N, so $x^N = 0$, whence $x = 0$. □

(ii) L f.d. algebra over F. If L contains no non-zero nilpotents, then by (i), $0 = P_1 \cap \cdots \cap P_r$ for prime ideals P_i of L. Moreover for $i \neq j$, $L = P_i + P_j$, because if P is a prime ideal, L/P is an integral domain, f.d. over F. If $x \in L/P$, $x \neq 0$, then mult^n by x is injective, hence surjective, hence x is invertible mod P. $\therefore L/P$ is a field. So P is maximal.

Hence $L \cong L/P_1 \times L/P_2 \times \cdots \times L/P_r$ by Chinese RT$_s$. and the L/P_i are fields, finite extensions of F.

$\therefore \Delta_{L/F} = \prod_i \Delta_{(L/P_i)/F} \neq 0$ if F is perfect.

Conversely if L contains a non-zero nilpotent element x, then $\forall\, y \in L$, $\mathrm{tr}(xy) = 0$. So $\Delta_{L/F} = 0$. $\square$

We are now in a position to prove Theorem 1. Recall this says that $\mathfrak{P} \trianglelefteq A$ (prime ideal) is ramified in $B \supseteq \mathfrak{P} \mid \Delta_{B/A}$.

Pf of Theorem 1.

We localise at $\mathfrak{P}$: write $A' = S^{-1}A$, $B' = S^{-1}B$ $(S = A \setminus \mathfrak{P})$. Then by Lemma 9.4, $\dfrac{B}{B\mathfrak{P}} \cong \dfrac{B'}{B'\mathfrak{P}}$, and by Lemma 2 above,

$\mathfrak{P}$ is ramified $\iff$ $\dfrac{B'}{B'\mathfrak{P}}$ contains a non-zero nilpotent elt.

So by Prop 4 (ii) above (with $F = A'/A'\mathfrak{P} = A/\mathfrak{P}$ and $L = B'/B'\mathfrak{P} = B/B\mathfrak{P}$) – a f.d. F-algebra –

$\mathfrak{P}$ is ramified $\iff$ $\Delta_{(B/\mathfrak{P}B')/(A'/A'\mathfrak{P})} = (0)$

Now A' is a PID, so B' is free of rank n over A'. Let $x_1, \ldots, x_n$ be an A'-basis of B', where $x_i \in B'$ $\forall i$.

Then by Lemma 3 above,

$\Delta_{(B'/B'\mathfrak{P})/(A'/A'\mathfrak{p})}(\bar{x}_1, \cdots, \bar{x}_n) = \Delta_{B'/A'}(x_1, \cdots, x_n) \neq (0)$

$\Leftrightarrow \Delta_{B'/A'}(x_1, \cdots, x_n) \in A'\mathfrak{P}$.

Suppose now that $y_1, \cdots, y_n$ is any K-basis of L which is contained in B. Then $y_i = \sum a'_{ij} x_j$ $(a'_{ij} \in A')$

and $\Delta_{K/L}(y_1, \cdots, y_n) = \det(a'_{ij})^2 \Delta_{K/L}(x_1, \cdots, x_n)$, & if

$\mathfrak{P}$ is ramified, $\Delta_{B/A}(y_1, \cdots, y_n) \in A'\mathfrak{P} \cap A = \mathfrak{p}$.

Hence $\mathfrak{P}$ is ramified $\Rightarrow \mathfrak{P} \mid \Delta_{B/A}$.

Conversely, if $\mathfrak{P} \supseteq \Delta_{B/A}$, then $\Delta_{B'/A'}(x_1, \cdots, x_n) \in A'\mathfrak{P}$, because if $x_i = \frac{y_i}{s}$ with $y_i \in B$ (recall $x_i \in B'$) then $\Delta(x_1, \cdots, x_n) = \frac{1}{s^{2n}} \Delta(y_1, \cdots, y_n)$

$\in S^{-1}\Delta_{B/A} \subseteq A'\mathfrak{P}$. Hence $\mathfrak{P}$ is ramified (see above). $\square$

Cor 1' Let K be an alg number fld, p a rational prime. Then p is ramified in $K \Leftrightarrow p \mid \Delta_{K/\mathbb{Q}}$.

Pf Take $K = \mathbb{Q}$, $L = K$ in Thm 1. Then p is ramified $\Leftrightarrow p \mid \Delta_{K/\mathbb{Q}} = d\mathbb{Z} \Leftrightarrow p \mid d$. $\square$

Cor 1'' Only finitely many primes of A are ramified in B.

Pf: $(\Delta_{B/A})$ has only finitely many prime divisors.

Examples (1) Quadratic fields. If $K = \mathbb{Q}(\sqrt{d})$ with d a square free integer then

(i) If $d \equiv 2$ or $3 \bmod 4$, then $\Delta = 4d$. Hence p is ramified $\Leftrightarrow p \mid 4d$. In particular, 2 is always ramified.

(ii) If $d \equiv 1 \bmod 4$, $\Delta = d$, so p is ramified $\Leftrightarrow p \mid d$.

(2) Cyclotomic fields. If $z =$ primitive p^{th} root of unity, $K = \mathbb{Q}(z)$, we have seen that $\Delta_{K/\mathbb{Q}} = \pm p^{p-2}$. Hence p is the unique prime which is ramified in K.

$N(\mathfrak{p}) = p^n$ $\quad (p) = \prod \mathfrak{p}_i^{e_i}$, $\quad \sum e_i f_i = n$.

Example - Decomposition of rational primes in quadratic fields

Take $A = \mathbb{Z}$, $K = \mathbb{Q}(\sqrt{d})$ $d \in \mathbb{Z}$ square free, $B =$ int. in K. For a rat'l prime p we shall determine the factorization of pB in B.

Theorem 1 of §9 tells us that

$$pB = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}, \text{ where } \mathfrak{p}_i \text{ is prime in } B \text{ and } \textstyle\sum_i e_i f_i = 2$$

Hence: $r \le 2$, and we seek solutions to $e_1 f_1 + e_2 f_2 = 2$. Hence pB has just 3 possible factorizations:

(i) $e_1 = e_2 = 1 = f_1 = f_2$: $pB = \mathfrak{p}_1 \mathfrak{p}_2$ - p decomposes.

(ii) $e_1 = 1$, $f_1 = 2$; $pB = \mathfrak{p}$ is prime - p is inert

(iii) $e_1 = 2$, $f_1 = 1$: $pB = \mathfrak{p}^2$. - p is ramified

We determine when the various cases occur. They are distinguished by the structure of B/pB. Moreover we've seen that (iii) happens $\Leftrightarrow p \mid \Delta_K = \Delta$.
So we suppose that $p \nmid \Delta$ and assume first that p is odd.

Now for $d \equiv 2$ or $3 \pmod 4$, $B = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$, so $B/pB \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}\sqrt{d}$.
Moreover for $d \equiv 1 \pmod 4$, $B = \frac{1}{2}(\mathbb{Z} + \mathbb{Z}\sqrt{d})$, where
$\mathbb{Z} + \mathbb{Z}\sqrt{d} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z},\ a \equiv b \pmod 2\}$.
$\therefore \frac{1}{2}(a + b\sqrt{d}) + \frac{p}{2}(a + b\sqrt{d}) = \frac{p+1}{2}(a + b\sqrt{d})$; so each coset in B/pB contains an elt $a + b\sqrt{d}$, $a, b \in \mathbb{Z}$.
Hence B/pB again $\cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}\sqrt{d}$.

So: $B/Bp \cong \dfrac{\mathbb{F}_p[t]}{\langle t^2 - \bar{d} \rangle}$, where $\bar{d}$ = residue class of $d \bmod p$.

Hence the cases correspond to the factorisation of $t^2 - \bar{d}$ over $\mathbb{F}_p$.
(i) $\leftrightarrow$ distinct roots, i.e. $\bar{d}$ is a square, $\neq 0 \bmod p$.
(ii) $\leftrightarrow$ $t^2 - \bar{d}$ is irred in $\mathbb{F}_p[t]$ — i.e. $\bar{d}$ is a non-square.
(iii) $\leftrightarrow$ $\bar{d} \equiv 0 \bmod p$. (note that for odd p, $p \mid \Delta \Leftrightarrow p \mid d$).

Now take $p = 2$.
If $d \equiv 2$ or $3 \bmod 4$, $\Delta = 4d$, so $p \mid \Delta$ and 2 is ramified.
[In detail: $B = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, so $B/2B \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\sqrt{d} \cong \mathbb{F}_2[t]/\langle t^2 - \bar{d} \rangle$
But $\bar{d}$ is always a square mod 2 ($\bar{d}^2 = \bar{d}$), so 2 is ramified].
If $d \equiv 1 \bmod 4$, $\Delta = d$ & B has basis $\frac{1}{2}(1 + \sqrt{d})$, $\frac{1}{2}(1 - \sqrt{d})$.
$\therefore B/2B = \mathbb{F}_2\left(\frac{1}{2}(1 + \sqrt{d})\right) \oplus \mathbb{F}_2\left(\frac{1}{2}(1 - \sqrt{d})\right)$.
$= \mathbb{F}_2(1) + \mathbb{F}_2\left(\frac{1}{2}(1 + \sqrt{d})\right)$.
$\cong \mathbb{F}_2[t] / \langle t^2 - t + \underbrace{\tfrac{1}{4}(1 - d)}_{\delta} \rangle$

Hence (i) $\Leftrightarrow$ f decomposes if $t^2 - t + \delta$ has distinct roots in $\mathbb{F}_2$; these roots must be $0, 1$ so $f(t) = t^2 - t$; so this happens $\Leftrightarrow \frac{1}{4}(1 - d) \equiv 0 \bmod 2$
i.e. $d \equiv 1 \bmod 8$.

$d \equiv 5 \bmod 8 \iff f(t)$ is irred $\iff$ case (iv) (2 is inert).

Summary: decomposed

(i) p is decomposed $\iff p = \beta_1 \beta_2$
- p is odd & d is a quadratic residue mod p.
- $p = 2$ and $d \equiv 1 \bmod 8$.

(ii) p is inert $\iff p = \mathfrak{p}$
- p is odd and d is a non-residue mod p
- $p = 2$ and $d \equiv 5 \bmod 8$

(iii) p is ramified $\iff p = \mathfrak{p}^2$
- p is odd and $d \equiv 0 \bmod p$.
- $p = 2$ and $d \equiv 2$ or $3 \bmod 4$.

---

§11 Galois extensions and Inertia groups.

When L is a Galois extension of K, we may obtain extra information about the e_i & f_i. (i.e. ramification index and residual degree).

Notation: as in §10, $A \subset K \subset L \subset \mathbb{C}$, with B the integral closure of A in L.

The additional assumption that L is a Galois extension of K, with $\mathrm{Gal}(L/K) = G$.

This means:
- Any K-hom $\sigma : L \hookrightarrow \mathbb{C}$ satisfies $\sigma(L) = L$.
- $L = K(\alpha)$ where and if $m_{K,\alpha}(t)$ is the minimal polynomial of α, then all roots of $m_\alpha(t)$ lie in L.

Note that for $\sigma \in G$, $\sigma B = B$ (since the equation of integral dependence does not change).

Let $\mathfrak{P}$ be a prime ideal of A. If $\mathfrak{p}$ is a prime ideal of B s.t. ~~$B \cap \mathfrak{p}$~~ $A \cap \mathfrak{p} = \mathfrak{P}$, the same is true of $\sigma\mathfrak{p}$. Hence if

$$B\mathfrak{P} = \prod_1^g \mathfrak{p}_i^{e_i},$$

G permutes the $\mathfrak{p}_i$. Further, $\mathfrak{p}$ & $\sigma\mathfrak{p}$ have the same e and f. Same e by unique factorization; same f, since $f = \dim_{A/\mathfrak{P}} B/\mathfrak{p} = \dim_{A/\mathfrak{P}} B/\sigma\mathfrak{p}$ ($\cdot\sigma$ is an isom).

Proposition 1. If $B\mathfrak{P} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$, G permutes the $\mathfrak{p}_i$ transitively; i.e.

given $\mathfrak{p}, \mathfrak{p}'$ s.t. $\mathfrak{p} \cap A = \mathfrak{p}' \cap A = \mathfrak{P}$, $\exists\, \sigma \in G$ s.t. $\mathfrak{p}' = \sigma\mathfrak{p}$.

Pf. Let $\mathfrak{p}$ be one of the $\mathfrak{p}_i$ which is $\cap A$ in the G-orbit of $\mathfrak{p}_1$. Then $\exists\, x \in \mathfrak{p}$ s.t. $x \notin \sigma(\mathfrak{p}_1)$ $\forall \sigma \in G$ (see subscript below). Then $N(x) = \prod_{\sigma \in G} \sigma(x) \in \mathfrak{p} \cap A = \mathfrak{P}$.

But $\forall \sigma$, $x \notin \sigma(\mathfrak{p}_1)$, i.e. $\sigma^{-1}(x) \notin \mathfrak{p}_1$. So $N(x) \notin \mathfrak{p}_1$, ✗.
Hence $\exists$ such a $\mathfrak{p}$, and G is transitive on the $\mathfrak{p}_i$. □

Cor 1. We have $B\mathfrak{P} = \left(\prod_{i=1}^{g} \mathfrak{p}_i\right)^e$ and $n = efg$.

Pf. All $\mathfrak{p}_i$ have the same e & f, & there are g of them. Since $\sum e_i f_i = n$, the result is clear. □

Sublemma. Let $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ be a set of prime ideals in R, $a \subseteq R$ such that $\forall i$, $\exists\, x_i \in a \setminus \mathfrak{P}_i$. Then $\exists\, x \in a$, $x \notin \mathfrak{P}_i$ $\forall i$. ($x \notin \bigcup \mathfrak{P}_i$).

Pf. $\exists\, a_i \in a \setminus \mathfrak{P}_i$ $\forall i$. Wlog no $\mathfrak{P}_i \subseteq \mathfrak{P}_j$; so $\exists\, x_{ij} \in \mathfrak{P}_j \setminus \mathfrak{P}_i$ $\forall i, j$. Let $x_i = a_i \prod_{j \neq i} x_{ij}$; $x_i \notin \mathfrak{P}_i$, $x_i \in \mathfrak{P}_j$ $\forall j \neq i$.

Then $x = x_1 + \cdots + x_r$ satisfies the condition. □

Defn. Let $D = \{\sigma \in G \mid \sigma\beta = \beta\}$ (for some $\beta = \beta_i$).
Then D is determined up to conjugacy in G & is called the decomposition group of the prime ideal β.

Lemma 2. $g = \frac{n}{|D|} \Rightarrow |D| = ef$. $\left(n = \sum_1^g e_i f_i = gef\right)$

Pf: Clearly at its side $= g = |G|/|D| = n/|D|$. □

LAST LECTURE

For $\sigma \in D$, $\sigma B = B$ $\sigma\beta = \beta$ so σ induces an automorphism of the field (finite) B/β over $A/\mathfrak{p}$. Thus we have a homomorphism

$$\alpha : D \to \mathrm{Aut}_{A/\mathfrak{p}}(B/\beta)$$

Defn. $\mathrm{Ker}(\alpha) := $ inertial group I of $\mathfrak{p}$.
It is determined up to conjugacy in G.

Theorem
Proposition 3. B/β is a Galois extension of $A/\mathfrak{p}$ of degree f and $\sigma \mapsto \alpha(\sigma)$ is a surjective homomorphism:

$$D \to \mathrm{Gal}(B/\beta \,/\, A/\mathfrak{p}).$$

In particular $|I| = e$. (since $\deg(B/\beta / A/\mathfrak{p}) = f$ and $|D| = ef$)

Proof. D is a subgroup of G. Let $L_D = \{a \in L \mid \sigma(a) = a \ \forall \sigma \in D\}$ be the corresponding intermediate field: $K \subset L_D \subset L$.
Then $\mathrm{Gal}(L/L_D) = D$.
Let $B_D = B \cap L_D$, the integral closure of A in L_D
$\mathfrak{P}_D = B_D \cap \beta$, a prime ideal of B_D which extends $\mathfrak{p}$.

By Prop 1, $D = \mathrm{Gal}(L/L_D)$ permutes the prime divisors of $\mathfrak{P}_D$ transitively. But β is one of them, and D fixes β. So

$$\mathfrak{P}_D = \beta^{e'}, \text{ and } \dim_{B_D/\mathfrak{P}_D}(B/\beta) = f', \text{ where}$$

$e'f' = |D| = ef$.

But $\mathfrak{P}_D = B_D \cap \mathfrak{p} \supseteq \mathfrak{P}$, so $\mathfrak{p}_D \supseteq B_D \mathfrak{P}$. Hence $B\mathfrak{P}_D \supseteq B\mathfrak{P}$, so that $\mathfrak{p}^{e'} \mid B\mathfrak{P}$, whence $e' \leq e$.

Similarly, $A/\mathfrak{P}$ is a subfield of $B_D/\mathfrak{P}_D$, whence $f' = \dim_{B_D/\mathfrak{P}_D} (D/\mathfrak{p}) \leq \dim_{A/\mathfrak{P}} (B/\mathfrak{p}) = f$.

Hence: $e = e'$ and $f = f'$. Thus we may replace L by L_D, G by D etc, and we are reduced to the case where $D = G$. We now assume this.

Now $B/\mathfrak{p}$ is a finite extension of $A/\mathfrak{P}$. Let $\bar{x} \in B/\mathfrak{p}$ be a generator, where $x \in B$ is a representative of $\bar{x}$.

Then x has a monic minimal polynomial $m(t)$ over A, and taking the coeffs modulo $\mathfrak{p}$ we obtain a polynomial all of whose roots are of the form $\overline{\sigma(x)}$ $(\sigma \in G)$. $(= \sigma(\bar{x}))$.

Hence $B/\mathfrak{p}$ is Galois over $A/\mathfrak{P}$. (H is the splitting field of $\overline{m(t)}$.) Moreover all automorphisms are given by $\bar{x} \mapsto \bar{\sigma}(\bar{x})$.

Thus $f = |G|/|I| = ef/|I|$, so that $|I| = e$. □.

(recall $I = \ker(G \to \mathrm{Aut}_{A/\mathfrak{P}}(B/\mathfrak{p}))$).

Case of number fields.

$K \subseteq L$ a Galois extension of number fields. If $\mathfrak{P} \subset A$ is unramified in B ($= \mathcal{O}_L$) then $T\left(\frac{B}{\mathfrak{P}'} / \frac{A}{\mathfrak{P}}\right) \cong D$, for any prime $\mathfrak{P}'$ of B with $\mathfrak{P}' \cap A = \mathfrak{P}$. Then $\frac{B}{\mathfrak{P}'}$ is a finite extension of the finite field $\frac{A}{\mathfrak{P}}$; if $\left|\frac{A}{\mathfrak{P}}\right| = q$, $\mathfrak{P}'$ then D is therefore cyclic, with distinguished generator the "Frobenius automorphism" $x \mapsto x^q$. $\left(x \in \frac{B}{\mathfrak{P}'}\right)$

Application to cyclotomic extensions. OMIT.

Theorem 4. Let $z \in \mathbb{C}$ be a primitive n^{th} root of unity.

(a) p ramifies in $\mathbb{Q}(z) \Rightarrow p \mid n$.

(b) $\mathbb{Q}(z)$ is a (Galois) cyclic extension of degree $\varphi(n)$ over $\mathbb{Q}$. Moreover $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Proof. (a) We need to compute the discriminant. For this we have seen that $D(1, z, z^2, \dots, z^{\varphi(n)-1}) = \pm\, m'(z)$, i.e. $\Delta_{\mathbb{Q}(z)/\mathbb{Q}} = \pm\, m'(z)$, where $m(z)$ is the minimal polynomial of z over $\mathbb{Q}$.

Now $t^n - 1 = m(t) \cdot f(t)$ for some $f(t) \in \mathbb{Z}[t]$

$\therefore\ n t^{n-1} = m'(t) f(t) + m(t) f'(t)$.

Aff. Substitute $t = z$: $\quad n z^{n-1} = m'(z) f(z) \qquad$ — (i)

Let $d = \text{degree } \mathbb{Q}(z)/\mathbb{Q} \ (= \varphi(n))$. Now taking norms in (i), using the fact that $N(z) = \pm 1$, we see

$n^d = m'(z) \times$ algebraic integer $\in \mathbb{Q}$.

In particular if $p \mid m'(z)$, then $p \mid n^d$, so $p \mid n$.

(b). The roots of $m(t)$ are powers z^i of z, where $\gcd(i, n) = 1$. There are $\varphi(n)$ of these, and $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q})$ permutes them cyclically (well known). $\square$

§12 Quadratic reciprocity

Legendre symbol This is a function denoted $(\ )$ or $(\ )_L$: $\mathbb{Z} \setminus p\mathbb{Z} \to \{\pm 1\}$, defined as follows: Let p be an odd prime.

$$d \mapsto \left(\frac{d}{p}\right) := \begin{cases} +1 & \text{if } d \text{ is a square (quadratic residue) mod } p \\ -1 & \text{if } d \text{ is not (i.e. is a quadratic non-residue mod } p. \end{cases}$$

May be described as follows: $\mathbb{Z} \setminus p\mathbb{Z} \to \mathbb{F}_p^* \to \mathbb{F}_p^* / (\mathbb{F}_p^*)^2 = \{\pm 1\}$.

[NB if $p = 2$ — this does not apply]

It follows that $\left(\frac{-}{p}\right)$ is multiplicative: $\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Lemma 1. (Euler's criterion) If p is an odd prime, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

If $\mathbb{F}_p^*$ is cyclic of order $p-1$. Hence $a^{p-1} \equiv 1 \bmod p$, and $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. If $a \equiv b^2 \bmod p$, then $a^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \bmod p$.

Conversely, $a^{\frac{p-1}{2}} = 1 \bmod p \Rightarrow a = b^{2k}$, b a generator of $\mathbb{F}_p^*$. □

Theorem 2 (Quadratic reciprocity) (Gauss). If p and q are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Proof. Let $K = \mathbb{Q}(z)$ where z is a primitive q^{th} root of unity (eg. $z = \exp\left(\frac{2\pi i}{q}\right)$). Then $[K : \mathbb{Q}] = q-1$ and

$\mathrm{Gal}(K/\mathbb{Q}) = G$ is cyclic, order $q-1$. Its elements are $\sigma_i : z \mapsto z^i$, $i = 1, 2, \dots, q-1$.

G has a unique subgroup H of index 2, so K has a unique quadratic subfield F, with $\mathrm{Gal}(K/F) = H$, so that $[F : \mathbb{Q}] = 2$.

Now we have seen that $\Delta_{K/F}\,\Delta_{F/\mathbb{Q}} = \Delta_{K/\mathbb{Q}} = \pm p^{p-2}$

Hence $\Delta_{F/\mathbb{Q}} \mid p^{p-2}$ $(*\neq 1)$, so $\Delta_{F/\mathbb{Q}} = p$ $(= p$ or $4p$, and $\neq 4p$ since $4 \nmid p^{p-2})$.

We now have

$$\begin{array}{ccccc} K = \mathbb{Q}(z) & \overset{\frac{q-1}{2}}{\supset} & F & \overset{2}{\supset} & \mathbb{Q} \\ \cup & & \cup & & \cup \\ B & \supset & A & \supset & \mathbb{Z} \end{array}$$

Now let $p \in \mathbb{Q}$ be prime. We have seen that $\Delta_K = \pm q^{q-2}$.
Hence p ramifies in $B \iff p = q$.
But $F = \mathbb{Q}\sqrt{d}$ for a square free integer d.
If p ramifies in F, then $pA = \mathfrak{p}^2$, where $\mathfrak{p}$ is prime in A.
So $pB = (\mathfrak{p}B)^2$ ramifies in K. Hence $p = q$. Hence the only (possible) prime which ramifies in F is $p = q$, whence:

$$F = \begin{cases} \mathbb{Q}(\sqrt{q}) & \text{if } q \equiv 1 \pmod 4 \\ \mathbb{Q}(\sqrt{-q}) & \text{if } q \equiv (2 \text{ or } 3) \bmod 4. \end{cases}$$

$\therefore F = \mathbb{Q}(\sqrt{q^*})$, where $q^* = (-1)^{\frac{q-1}{2}}$

Now by §4 Thm 2, the integers $B = \mathbb{Z}[z]$. If $p \in \mathbb{Z}$ is an odd prime, distinct from q, then p is unramified in B, so $pB = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, with $\mathfrak{p}_i$ prime in B. Write $\mathfrak{p} = \mathfrak{p}_1$, and let $\sigma_{\mathfrak{p}}$ be the Frobenius automorphism of $B/\mathfrak{p}$; consider the restriction of $\sigma_{\mathfrak{p}}$ to A/pA. This restriction is trivial (i.e. $= \mathrm{id}_{A/pA}$) $\iff \sigma_{\mathfrak{p}} \in \left(F_q^*\right)^2 \iff p$ is a square mod $q \iff \left(\frac{p}{q}\right) = 1$.

But p decomposes in $A \iff t^2 - q^*$ decomposes mod p
$\iff q^*$ is a square mod p

(Galois trivially in $\mathrm{Gal}(A/\mathbb{Z})$).

It followed that $\left(\frac{p}{q}\right) = 1 \iff \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) = 1$, i.e.

$\therefore$ if $\left\{\frac{q-1}{2}\right\}$ is even, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$
$\left\{\frac{p-1}{2}\right\}$

If $\frac{p-1}{2}, \frac{q-1}{2}$ are odd, then -1 is a non-square mod p & mod q.

Hence $\left(\frac{q}{p}\right) = 1 \Rightarrow \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) = -1 \Rightarrow \left(\frac{p}{q}\right) = -1$. □

[NB: need both $(-1)^{\frac{p-1}{2}}, (-1)^{\frac{q-1}{2}} = -1$ because we gives that (-1) is a non-square mod p & the other gives a coeff -1.]