PMATH 441/641 ALGEBRAIC NUMBER THEORY

1. Lecture: Wednesday, January 5, 2000

NO TEXT
References:

- Number Fields (Marcus)
- Algebraic Number Theory (Lang) (Stewart & Hill)

Marks:

- Final Exam 65%
- Midterm 25%
- Assignments 10%

Definition. An *algebraic integer* is the root of a monic polynomial in $\mathbb{Z}[x]$.
An *algebraic number* is the root of any non-zero polynomial in $\mathbb{Z}[x]$.

We are interested in studying the structure of the ring of algebraic integers in an algebraic number field. A number field is a finite extension of $\mathbb{Q}$. We'll assume that the number fields we consider are all subfields of $\mathbb{C}$.

Definition. Suppose that K and L are fields with $K \subseteq L$. Then K is a *subfield* of L and L is an *extension field* of K.
We denote the dimension of L as a vector space over K by $[L : K]$.
If $[L : K] < \infty$, we say L is a *finite extension* of K.

Definition. Suppose that H is a field with $K \subseteq H \subseteq L$. Then we say H is an *intermediate field* of K and L. Recall that $[L : K] = [L : H][H : K]$.

Definition. A polynomial $f \in K[x]$ is said to be *irreducible* over K iff whenever $f = gh$ with $g, h \in K[x]$, we have g or h constant.

Recall that $K[x]$ is a Principal Ideal Domain.

Definition. Let K be a subfield of $\mathbb{C}$ and let $\theta \in \mathbb{C}$ be an algebraic number. We denote by $K(\theta)$ the smallest subfield of $\mathbb{C}$ containing K and θ,

Definition. Let K be a subfield of $\mathbb{C}$ and let $\theta \in \mathbb{C}$ to be algebraic over K. A polynomial in $K[x]$ is said to be a *minimal polynomial* of θ over K if it is monic, has θ as a root, and has degree as small as possible with these properties.

Theorem 1. *Let $K \subseteq \mathbb{C}$. Let $\theta \in \mathbb{C}$ be algebraic over K. Then there is a unique minimal polynomial of θ over K.*

Proof:
Plainly there is at least one. Suppose that $p_1(x)$ and $p_2(x)$ are minimal polynomials for θ over K.
Consider $p_1(x) - p_2(x)$. Since p_1, p_2 are monic and of minimal degree, the degree of $p_1(x) -$

$p_2(x)$ is strictly smaller than the degree of $p_1(x)$, or $p_1(x) = p_2(x)$.
In the former case, we contradict the minimality of the degree since $p_1(\theta) - p_2(\theta) = 0$. Thus $p_1 = p_2$ and the result follows. □

Thus we can speak of "the" minimal polynomial of θ over K.

Definition. Let $K \subseteq \mathbb{C}$. Let θ be algebraic over K. The *degree of θ over K* is the degree of the minimal polynomial of θ over K.

Remark. Let $K \in \mathbb{C}$ and $\theta \in \mathbb{C}$ with θ algebraic over K. Let $p(x)$ be the minimal polynomial of θ over K. Suppose $f \in K[x]$ with $f(\theta) = 0$. Then $p \mid f$ in $K[x]$. To see this note that by the Division Algorithm in $K[x]$,

$$f(x) = q(x)p(x) + r(x) \text{ with } r = 0 \text{ or } \deg r < \deg p$$

and $q, r \in K[x]$. But

$$f(\theta) = q(\theta)p(\theta) + r(\theta)$$

Thus $r(\theta) = 0$. If r is not identically zero, then p would not have minimal degree and so $r = 0$. Then $p = f$ in $K[x]$.

Theorem 2. *Let $K \subseteq \mathbb{C}$. If $f \in K[x]$ is irreducible in $K[x]$ of degree n, then f has n distinct roots in $\mathbb{C}$.*

Proof:
Suppose that in $\mathbb{C}[x]$,

$$f(x) = a_n(x - \alpha)^2 f_1(x)$$

with $a_n \in \mathbb{C}$, $\alpha \in \mathbb{C}$, $f_1 \in \mathbb{C}[x]$. Then

$$f'(x) = 2a_n(x - \alpha)f_1(x) + a_n(x - \alpha)^2 f_1'(x)$$

In particular, $f'(\alpha) = 0$.
Let p be the minimal polynomial of α over K. Then p divides f and f'.
Thus f is not irreducible. The contradiction establishes the result. □

---

2. Lecture: Friday, January 7, 2000

Let $\theta \in \mathbb{C}$ and suppose that θ is algebraic over a field K ($K \subseteq \mathbb{C}$).

Definition. Let $p(x)$ be the minimal polynomial of θ over K (i.e. $p \in K[x]$). Let $\theta = \theta_1, \ldots, \theta_n$ be the roots of p. $\theta = \theta_1, \ldots, \theta_n$ are known as the *conjugates of θ over K*. When $K = \mathbb{Q}$ we just refer to the *conjugates of θ*.

Theorem 3. *Let $K \subseteq \mathbb{C}$ and let $\theta \in \mathbb{C}$ be algebraic over K of degree n. Every element α in $K(\theta)$ has a unique representation in the form*

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + \ldots + a_{n-1}\theta^{n-1} = r(\theta)$$

with $a_0, a_1, \ldots, a_{n-1} \in K$.

Proof:

Existence: We have $K(\theta) = \{\frac{f(\theta)}{g(\theta)} : f, g \in K[x], g(\theta) \neq 0\}$. Let $\alpha \in K(\theta)$. Then $\alpha = \frac{f(\theta)}{g(\theta)}$.
Let p be the minimal polynomial for θ over K.
Then p and g are coprime and so there exist $s, t \in K[x]$ with $s(x)p(x)+t(x)g(x) = 1$.
Thus $t(\theta)g(\theta) = 1$. Hence $\alpha = f(\theta)t(\theta)$.
Next, by the Division Algorithm,

$$f(x)t(x) = q(x)p(x) + r(x) \text{ with } q, r \in K[x] \text{ and } r = 0 \text{ or } \deg r \leq n-1$$

But then $f(\theta)t(\theta) = r(\theta)$ hence $\alpha = r(\theta)$, as required.
Uniqueness: Suppose $\alpha = r_1(\theta)$ and $\alpha = r_2(\theta)$, with $r_1, r_2 \in K[x]$ of degree $\leq n-1$.
Then $r_1(x) - r_2(x)$ is zero or has degree $\leq n-1$.
But $r_1(\theta) - r_2(\theta) = 0$ and θ has degree n over K.
Thus $r_1(x) = r_2(x)$, as required.

□

Note that $K(\theta) = K[\theta]$.

Definition. Let R and S be rings. An injective homomorphism $\varphi : R \to S$ is said to be an *embedding* of R in S.

Theorem 4. *Let K be a subfield of $\mathbb{C}$ and let L be a finite extension of K. Every embedding of K in $\mathbb{C}$ extends to exactly $[L : K]$ embeddings of L in $\mathbb{C}$.*

Proof:
We prove this by induction on $[L : K]$:
If $[L : K] = 1$, then the result is immediate.
Suppose that $[L : K] > 1$. Let σ be an embedding of K into $\mathbb{C}$.
Let $\alpha \in L \setminus K$. Let $p(x)$ be the minimal polynomial of α over K.
If $p(x) = a_m x^m + \ldots + a_0$, let $g(x) = \sigma(a_m)x^m + \ldots + \sigma(a_0)$. Then g is irreducible over $\sigma(K)$.
Let $\beta_1, \ldots, \beta_m$ be the roots of g in $\mathbb{C}$. For each root β of g we define the map $\lambda_\beta : K[\alpha] \to \mathbb{C}$ by

$$\lambda_\beta(b_0 + b_1\alpha + \ldots + b_{m-1}\alpha^{m-1}) = \sigma(b_0) + \sigma(b_1)\beta + \ldots + \sigma(b_{m-1})\beta^{m-1}$$

We can check that λ_β is a ring homomorphism which extends σ. We have m distinct roots β of g and so m embeddings of $K(\alpha)$ in $\mathbb{C}$ which extend σ.
Further, there are no other such embeddings λ since $0 = \lambda(0) = \lambda(p(\alpha)) = g(\lambda(\alpha))$, and we see that $\lambda(\alpha)$ is a root of g.
We now appeal to our inductive hypothesis. Each of the m embeddings of $K(\alpha)$ in $\mathbb{C}$ extend to $[L : K(\alpha)]$ embeddings of L in $\mathbb{C}$ and so we have $[L : K(\alpha)][K(\alpha) : K] = [L : K]$ embeddings of L in $\mathbb{C}$ extending σ.
The result now follows (by induction). □

Theorem 5. *Let $K \subseteq L \subseteq \mathbb{C}$. Suppose that L is a finite extension of K. Then there is a $\theta \in L$ such that $L = K(\theta)$.*

Proof:
Since L is a finite extension of K, there exist algebraic numbers $\alpha'_1, \ldots, \alpha'_{n'}$ such that $L = K(\alpha'_1, \ldots, \alpha'_{n'})$.

By induction it suffices to show that when $n' = 2$ we can find θ such that $L = K(\theta)$.
Suppose that $L = K(\alpha, \beta)$ with α, β algebraic over K.
Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over K and let $\beta = \beta_1, \ldots, \beta_m$ be the conjugates of β over K.
For each $i \neq 1$ and k we consider the equation $\alpha_1 + x\beta_1 = \alpha_i + x\beta_k$.
The linear equation has 1 solution. Choose $c \in K, c \neq 0$ to avoid all such solutions. (Such a choice is possible since K is infinite).
Put $\theta = \alpha + c\beta = \alpha_1 + c\beta_1$. Plainly $K(\theta) \subseteq K(\alpha, \beta)$.

Thus, it remains to show that α, β are in $K(\theta)$, hence that $K(\alpha, \beta) \subseteq K(\theta)$.
Since $\alpha = \theta - c\beta$, it suffices to show that $\beta \in K(\theta)$.
Let $f(x)$ be the minimal polynomial of α over K.
Let $g(x)$ be the minimal polynomial of β over K. Notice that β is a root of the polynomial $f(\theta - cx)$ since $f(\theta - c\beta) = f(\alpha) = 0$.
Observe, by our choice of c, that β is the only common root of $f(\theta - cx)$ and $g(x)$.
Let h be the minimal polynomial of β over $K(\theta)$. Note that $f(\theta - cx)$ and $g(x)$ are in $K(\theta)[x]$.
Thus h divides $f(\theta - cx)$ and h divides $g(x)$ in $K(\theta)[x]$.
Since the only common root of $f(\theta - cx)$ and $g(x)$ is β, we conclude that h is linear.
Therefore there exist $\gamma_1, \gamma_2 \in K(\theta)$ with $\gamma_1 \neq 0$ such that $\gamma_1\beta + \gamma_2 = 0$.
Therefore $\beta \in K(\theta)$, as required.
(The result follows by induction.) □

3. Lecture: Monday, January 10, 2000

Definition. Let $K \subseteq L \subseteq \mathbb{C}$. We say that L is a *normal extension* of K if L is closed under the process of taking conjugates over K.

Theorem 6. *Let $K \subseteq L \subseteq \mathbb{C}$ with $[L : K] < \infty$. L is normal over K if and only if every embedding of L in $\mathbb{C}$ which fixes each element of K is an automorphism of L.*

Proof:

($\Rightarrow$) By Theorem 5 there exists an $\alpha \in$ Ł such that $L = K(\alpha) = K[\alpha]$.
Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over K.
There are n embeddings of L in $\mathbb{C}$ which fix K and they are given by $\lambda_1, \ldots, \lambda_n$ where $\lambda_i(\alpha) = \alpha_i$ for $i = 1, \ldots, n$, and $\lambda_i(t) = t$ for all $t \in K$.
Since L is normal, it is closed under taking conjugates over K and so $\alpha_1, \ldots, \alpha_n$ are in L.
Thus $\lambda_i : L \to L$ and so λ_i is an automorphism of L for $i = 1, \ldots, n$.

($\Leftarrow$) Let $\alpha \in L$. Consider $K[\alpha]$.
Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over K.
By Theorem 4, every embedding of $K[\alpha]$ in $\mathbb{C}$ extends to an embedding of L in $\mathbb{C}$.
Each such embedding is an automorphism by assumption.
Further, the embeddings of $K[\alpha]$ in $\mathbb{C}$ which fix K have the property that α is taken to a conjugate of α.
Furthermore, there is an embedding for *each* conjugate of α.
Therefore, each conjugate of α is in L, hence L is normal.

□

Remark. By Theorem 4, there are $[L : K]$ embeddings of L in $\mathbb{C}$ which fix each element of K.
By Theorem 6, L is normal over K iff there are $[L : K]$ automorphisms of L which fix each element of K.

Theorem 7. *Let $K \subseteq \mathbb{C}$. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be in $\mathbb{C}$ with $\alpha_1, \ldots, \alpha_n$ algebraic over K. Put $L = K(\alpha_1, \ldots, \alpha_n)$.*
If the conjugates of $\alpha_1, \ldots, \alpha_n$ over K are in L, then L is normal over K.

Proof:
We have $K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$.
By Theorem 5, $L = K[\theta]$, where $\theta = f(\alpha_1, \ldots, \alpha_n)$ with $f \in K[x_1, \ldots, x_n]$.
Let σ be an embedding of L in $\mathbb{C}$ which fixes each element of K. Then $\sigma\theta = f(\sigma\alpha_1, \ldots, \sigma\alpha_n)$.
Since $\sigma\alpha_i$ is an conjugate of α_i for $i = 1, \ldots, n$ and since each conjugate of α_i is in L, we conclude that $\sigma\theta$ is in L.
Therefore, σ is an automorphism of L. Thus, by Theorem 6, L is normal over K. □

Corollary 8. *Let $K \subseteq \mathbb{C}$ and let $L \subseteq \mathbb{C}$ with $[L : K]$ finite. There is a finite extension H of L, with $H \subseteq \mathbb{C}$ for which H is normal over K.*

Proof:
By Theorem 5, there is a $\theta \in L$ for which $L = K(\theta)$.
Let $\theta = \theta_1, \ldots, \theta_n$ be the conjugates of θ over K. Put $H = K(\theta_1, \ldots, \theta_n)$.
By the result of Theorem 7, H is normal over K. Plainly, H contains K. □

Remark. H is also normal over L, e.g. take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$.
Then L is not a normal extension of $\mathbb{Q}$ since the map $\sigma : L \to \mathbb{Q}$ given by

$$\sigma(t) = t \text{ for all } t \in \mathbb{Q} \text{ and}$$
$$\sigma(\sqrt[3]{2}) = w\sqrt[3]{2} \text{ where } w = e^{\frac{2\pi i}{3}}$$

is an embedding. However $w\sqrt[3]{2} \notin \mathbb{R}$ and so $w\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$. Therefore, σ is not an automorphism of L hence L is not a normal extension of $\mathbb{Q}$.
Put $H = \mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2})$.
Then H is a normal extension of $\mathbb{Q}$.
Observe that $H = \mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2})$ so $[H : L] = 2$.

---

4. Lecture: Wednesday, January 12, 2000

Definition. Let $K \subseteq L \subseteq \mathbb{C}$, with $[L : K] < \infty$. We define the *Galois group* of L over K, denoted by $\mathrm{Gal}(L/K)$, to be the set of automorphisms of L which fix each element of K.
The binary operation on the set is composition.
The identity element of the group is the identity map.
By Theorem 4 and Theorem 6, L is normal over K if and only if

$$|\mathrm{Gal}(L/K)| = [L : K]$$

Definition. Let H be a subgroup of $\mathrm{Gal}(L/K)$. We define the *fixed field* F_H of H to be the field $\{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$.
This is indeed a field since if α, β are in F_H, then so are $\alpha\beta^{-1}$ and $\alpha - \beta$.

Theorem 9. *Let $K \subseteq L \subseteq \mathbb{C}$ with $[L : K] < \infty$.*
Suppose that L is a normal extension of K. Let G be the Galois group of L over K. K is the fixed field of G and K is not the fixed field of any proper subgroup of G.

Proof:
Certainly K is fixed by every element of G. Suppose that $\alpha \in L$ and α is in the fixed field of G. Then $K(\alpha)$ is in the fixed field of G.
Since L is a normal extension of K, we have, by Theorem 4 and 6, that $|G| = [L : K]$. Thus there are $[L : K]$ embeddings of L in $\mathbb{C}$ which fix $K(\alpha)$. Since $[L : K] = [L : K(\alpha)][K(\alpha) : K]$ we see that $[K(\alpha) : K] = 1$ hence $\alpha \in K$. Therefore K is in the fixed field of G.

Let H be a proper subgroup of G and suppose that K is in the fixed field of H. Let $L = K[\alpha]$ for $\alpha \in L$. Consider

$$f(x) = \prod_{\sigma \in H} (x - \sigma\alpha)$$
$$f(x) = x^{|H|} - s_1(\sigma\vec{\alpha})x^{|H|-1} + \ldots + (-1)^{|H|}s_{|H|}(\sigma\vec{\alpha})$$

where $\sigma\vec{\alpha} = (\sigma_1(\alpha), \dots, \sigma_{|H|}(\alpha))$ are the elements of H.
Further $s_1, \dots, s_{|H|}$ are the elementary symmetric functions in the variables $x_1, \dots, x_n$ so that

$$\begin{aligned} s_1(x_1, \dots, x_{|H|}) &= x_1 + \cdots + x_{|H|} \\ s_2(x_1, \dots, x_{|H|}) &= x_1x_2 + x_2x_3 + \cdots + x_{|H|-1}x_{|H|} \\ &\vdots \\ s_{|H|}((x_1, \dots, x_{|H|}) &= x_1 \cdots x_{|H|} \end{aligned}$$

Notice that $\sigma s_i(\sigma\vec{\alpha}) = s_i(\sigma\vec{\alpha})$ for $i = 1, \dots, |H|$ and for all $\sigma \in H$. Thus, since K is the fixed field of H we see that $f \in K[x]$.
Therefore the minimal polynomial of α over K divides f, hence

$$[L : K] = [K(\alpha) : K] \leq \deg f = |H| < |G| = [L : K] \text{ (since L is normal over K)}$$

This contradiction completes the proof. □

Suppose that $K \subseteq L \subseteq \mathbb{C}$, $[L : K] < \infty$ and L is normal over K. Let G be the Galois group of L over K.
Let S_1 be the set of fields F with $K \subseteq F \subseteq L$.
Let S_2 be the set of subgroups H of G.
We define $\lambda : S_1 \to S_2$ by $\lambda(F) = \text{Gal}(L/F)$.
We define $\mu : S_2 \to S_1$ by $\mu(H) = F_H$ (the fixed field of H).

Theorem 10 (Fundamental Theorem of Galois Theory)**.** *μ and λ are inverses of each other. Suppose that $\lambda(F) = H$. Then F is normal over K if and only if H is a normal subgroup of G.*
Further, if F is normal over K, then there is an isomorphism $\delta : G/H \to \text{Gal}(F/K)$ given by $\delta(\sigma + H) = \sigma'$, where σ' is the automorphism of F which fixes K induced by σ.

Proof:
We first prove that μ and λ are inverses. Notice that

$$\mu \circ \lambda(F) = \mu(\text{Gal}(L/F)) = \text{ fixed field of Gal}(L/F)$$

and so by Theorem 9, $\mu \circ \lambda(F) = F$. Then $\mu \circ \lambda = id$.
Next note that $\lambda \circ \mu(H) = \lambda(F_H) = \text{Gal}(L/F_H)$.
Let $H' = \text{Gal}(L/F_H)$. By Theorem 9, F_H is the fixed field of H' and is not the fixed field of any proper subgroup of H'. Thus $H' \subseteq H$.
But if $\sigma \in H$, then σ is an automorphism of L fixing F_H and so σ is in $\text{Gal}(L/F_H)$.
Thus $H \subseteq H'$ and so $H = H'$. Thus $\lambda \circ \mu = id$.
Observe that if $H = \text{Gal}(L/F)$ and $\gamma \in H, \sigma \in G$ then $\sigma \circ \gamma \circ \sigma^{-1} \in \text{Gal}(L/\sigma F)$. Further, if $\theta \in \text{Gal}(L/\sigma F)$ then $\sigma^{-1} \circ \gamma \circ \sigma \in \text{Gal}(L/\sigma F) = H$. Thus $\text{Gal}(L/\sigma F) = \sigma H \sigma^{-1}$.
Next, note that F is normal over K if and only if every embedding of F in $\mathbb{C}$ which fixes K is an automorphism of F.
Each such embedding extends to an element of $\text{Gal}(L/K) = G$.

Thus F is normal $\iff \sigma F = F$ for all $\sigma \in G \iff \sigma H \sigma^{-1} = H$ for all $\sigma \in G \iff H \trianglelefteq G$

Let us now assume that F is a normal extension of K.
Consider the group homomorphism λ given by

$$\lambda : G = \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$$

by $\lambda(\sigma) = \sigma_{|F}$ (This is well-defined since F is a normal extension of K).
The map is certainly surjective, since every element of $\mathrm{Gal}(F/K)$ extends to an element of G. Further, the kernel of λ is $\mathrm{Gal}(L/F)$.
By the First Isomorphism Theorem (for Groups),

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/F)} \cong \mathrm{Gal}(F/K)$$

□

---

5. Lecture: Friday, January 14, 2000

Recall that an algebraic integer is the root of a monic polynomial in $\mathbb{Z}[x]$.

Theorem 11. *Let α be an algebraic integer. The minimal polynomial of α over $\mathbb{Q}$ is in $\mathbb{Z}[x]$.*

Proof:
Since α is an algebraic integer, then α is a root of some monic polynomial $h \in \mathbb{Z}[x]$. Let f be the minimal polynomial of α.
Then $h = f \cdot g$ with $f, g \in \mathbb{Q}[x]$. But f is monic, and so g is monic.
Choose $a, b \in \mathbb{Z}$ so that $af, bg \in \mathbb{Z}[x]$ and are primitive, i.e. have content 1.
Thus $abh = (af)\cdot(bg)$. By Gauss' Lemma, the product of primitive polynomials (in a Unique Factorization Domain) is primitive and so $a \cdot b = 1$.
Thus $f \in \mathbb{Z}[x]$. □

Remark. The only algebraic integers in $\mathbb{Q}$ are the ordinary integers.

Corollary 12. *Let d be a squarefree integer. The set of algebraic integers in $\mathbb{Q}[\sqrt{d}]$ is*

$$\begin{cases} \{r + s\sqrt{d} \mid r, s \in \mathbb{Z}\} & \text{when } d \equiv 2 \text{ or } 3 \pmod 4 \\ \{\frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2\} & \text{when } d \equiv 1 \pmod 4 \end{cases}$$

Proof:
Let $\alpha = r + s\sqrt{d}$ be in $\mathbb{Q}(\sqrt{d})$ so r, s are in $\mathbb{Q}$.
If $s = 0$ then $r \in \mathbb{Z}$. Suppose $s \neq 0$. Then the minimal polynomial of α over $\mathbb{Q}$ is given by

$$(x - (r + s\sqrt{d}))(x - (r - s\sqrt{d})) = x^2 - 2rx + r^2 - ds^2 \in \mathbb{Q}[x]$$

By Theorem 11, $f \in \mathbb{Z}[x]$. Thus $2r$ and $r^2 - ds^2$ are integers.
Note that if r is an integer, s is also an integer.
The other possibility is that $r = \frac{a}{2}$ with a an integer $\equiv 1 \pmod 2$. Then, since $r^2 - ds^2$ is an integer, we see then $s = \frac{b}{2}$ with $b \equiv 1 \pmod 2$ and $a^2 - db^2 \equiv 0 \pmod 4$
In this case we have $d \equiv 1 \pmod 4$. □

We want to prove next that the set of all algebraic integers forms a ring, and that the set of algebraic integers in any finite extension of $\mathbb{Q}$ forms a ring.
We need to show that if α, β are algebraic integers then so are $\alpha\beta$ and $\alpha + \beta$.

6. Lecture: Monday, January 17, 2000

Theorem 13. *Let α be a complex number. Then the following are equivalent:*

i) *α is an algebraic integer.*
ii) *the additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated.*
iii) *α is a member of some subring of $\mathbb{C}$ having a finitely generated additive group.*
iv) *$\alpha A \subseteq A$ for some finitely generated additive subgroup A of $\mathbb{C}$.*

Proof:

[i) $\Rightarrow$ ii)]: by Theorem 4 since $\mathbb{Z}[\alpha] = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Z}\}$ where n is the degree of α over $\mathbb{Q}$.
[ii) $\Rightarrow$ iii)]: immediate
[iii) $\Rightarrow$ iv)]: immediate
[iv) $\Rightarrow$ i)]: Suppose that $a_1, \ldots, a_n$ generate A.
Since $\alpha A = A$, we have $\alpha a_i = m_{i,1}a_1 + \cdots + = m_{i,n}a_n$ for some integers $m_{i,1}, \ldots, m_{i,n}$, for $i = 1, \ldots, n$.
Thus $(\alpha I_n - M)\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Since $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ we have $\det(\alpha I_n - M) = 0$.
Therefore, α is the root of a monic polynomial with integer coefficients.
Thus α is an algebraic integer.

□

Corollary 14. *If α and β are algebraic integers, then $\alpha + \beta$ and $\alpha\beta$ are algebraic integers.*

Proof:
Suppose that α has degree n and β has degree m.
Observe that $\mathbb{Z}[\alpha, \beta]$ is generated by $\{\alpha^i\beta^j \mid i = 0, \ldots, n-1, j = 0, \ldots, m-1\}$ over $\mathbb{Z}$.
Plainly $\alpha\beta$ and $\alpha + \beta$ are in $\mathbb{Z}[\alpha, \beta]$ and so the result follows from i) and iii) of Theorem 13. □

Theorem 15. *Let α be an algebraic number. There is a positive integer r such that $r\alpha$ is an algebraic integer.*

Proof:
Since α is an algebraic number, α is a root of a polynomial

$$q(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$$

with $b_{n-1}, \ldots, b_0 \in \mathbb{Q}$. Clear the denominators to obtain a polynomial $h(x) = a_n x^n + \cdots + a_0$ with $a_0, \ldots, a_n \in \mathbb{Z}$ such that $h(\alpha) = 0$. Thus ${a_n}^{n-1}h(\alpha) = 0$ and

$${a_n}^{n-1}h(x) = (a_n x)^n + a_{n-1}(a_n x)^{n-1} + \cdots + a_1{a_n}^{n-2}(a_n x) + a_0{a_n}^{n-1} \in \mathbb{Z}[x]$$

Therefore there is an nonzero integer r such that $r\alpha$ is an algebraic integer. Since whenever β is an algebraic integer, so is $-\beta$, the result follows. □

By Corollary 14 and the second property above, we see that the set of algebraic integers is a subring of $\mathbb{C}$.
Let $\mathbb{A}$ denote the ring of algebraic integers. For any finite extension K of $\mathbb{Q}$, let $\mathbb{A} \cap K$ be the ring of algebraic integers of K.
$\mathbb{A} \cap K$ is also known as the number ring of K.
We have already determined the number ring of each quadratic extension of $\mathbb{Q}$. We'll now determine the ring of algebraic integers of K when K is a cyclotomic extension $\mathbb{Q}$, i.e. an extension of $\mathbb{Q}$ by a root of unity.
Let $n \in \mathbb{Z}^+$ and put $\zeta_n = e^{\frac{2\pi i}{n}}$.
The cyclotomic extensions $\mathbb{Q}(\zeta_n), n = 1, 2, \ldots$ are fundamental in the following sense. They are Galois extensions of $\mathbb{Q}$ with abelian Galois groups.
Further, any normal extension of $\mathbb{Q}$ with an abelian Galois group is a subfield of $\mathbb{Q}(\zeta_n)$ for some n.
We'll prove the former assertion but not the latter.
For any positive integer n, we define $\Phi_n(x)$, the nth cyclotomic polynomial, by

$$\Phi_n(x) = \prod_{\substack{j=1, \\ (j,n)=1}}^{n} (x - \zeta_n^j)$$

---

7. Lecture: Wednesday, January 19, 2000

Theorem 16. *$\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$, for $n = 1, \ldots$*

Proof:
We'll show that $\zeta_n^j, j = 1, \ldots, n$ with $(j, n) = 1$ are all the conjugates of ζ_n or equivalently that Φ_n is the minimal polynomial of ζ_n.
ζ_n is a root of $x^n - 1$ and is therefore an algebraic integer. Thus if we show that Φ is the minimal polynomial of ζ_n, we conclude that $\zeta_n \in \mathbb{Z}[x]$.
Let $r(x)$ be the minimal polynomial of ζ_n over $\mathbb{Q}$. Since ζ_n is a root of $x^n - 1$, then $r(x) \mid x^n - 1$ in $\mathbb{Q}[x]$. The roots of $x^n - 1$ are the n different nth roots of 1 in $\mathbb{C}$ and so the roots of $r(x)$ are of the form ζ_n^k for some $k \in \mathbb{Z}^+$.
Observe that if $(n, k) > 1$, then ζ_n^k is a root of $x^{\frac{n}{(n,k)}} - 1$. Since ζ_n is not a root of $x^{\frac{n}{(n,k)}} - 1$ we see that in this case ζ_n^k is not a conjugate of ζ_n.
Thus the only possible conjugates are those of the form ζ_n^j; with $j = 1, \ldots, n$ and $(j, n) = 1$.
To show this, it suffices to prove that if $\theta = \zeta_n^t$ for some positive integer t which is coprime with n then, for each prime p which is coprime with n, θ^p is a conjugate of θ.
We then show that ζ_n^j is a conjugate of ζ_n^j by factoring j into prime factors and repeatedly appending the result.
Accordingly, let $f(x)$ be the minimal polynomial of θ over $\mathbb{Q}[x]$. Thus there exists $g(x) \in \mathbb{Q}[x]$ which is monic, such that

$$x^n - 1 = f(x)g(x)$$

By Gauss' lemma, f, g are in $\mathbb{Z}[x]$.
Since θ^p is a root of $x^n - 1$, it is a root of either $f(x)$ or $g(x)$.
If θ^p is a root of $f(x)$, then it is a conjugate of θ, as required. Suppose then that θ^p is a root

of $g(x)$. Then θ is a root of $g(x^p)$. Thus $f(x) \mid g(x^p)$ in $\mathbb{Q}[x]$, hence in $\mathbb{Z}[x]$.

For any $h(x) = a_0 + a_1x + \ldots + a_nx^n$ in $\mathbb{Z}[x]$, we define the *reduction* of h mod p, denoted by $\overline{h}(x)$, to be polynomial in $(\mathbb{Z}/p\mathbb{Z})[x]$ by

$$\overline{h}(x) = \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_nx^n$$

where for any integer a, $\overline{a} = a + p\mathbb{Z}$.
Note that the mapping $\mu : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ given by $\mu(h) = \overline{h}$, is a ring homomorphism.
Further, $\overline{h}(x^p) = \overline{h(x)}^p$ since

$$\overline{h}(x^p) = \overline{a}_0 + \overline{a}_1(x^p) + \cdots + \overline{a}_r(x^p)^r = \overline{a}_0{}^p + \overline{a}_1{}^p(x^p) + \cdots + \overline{a}_r{}^p(x^p)^r = \overline{h(x)}^p$$

Thus since $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$, we see that $\overline{f}$ divides $\overline{g}(x^p)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$, and so divides $(\overline{g}(x))^p$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.
Since $(\mathbb{Z}/p\mathbb{Z})[x]$ is a Unique Factorization Domain, there is an irreducible polynomial $s(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ which divides $\overline{f}$ and so also $\overline{g}$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.
But $x^n - 1 = f(x)g(x)$ in $\mathbb{Z}[x]$, hence $x^n - \overline{1} = \overline{f}(x)\overline{g}(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.
Thus $s(x)^2 \mid x^n - \overline{1}$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ and so $s(x) \mid \overline{n}x^{n-1}$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.
Since p and n are coprime, then $\overline{n}x^{n-1}$ is not the zero polynomial. Thus $s(x) = cx$ for some nonzero $c \in (\mathbb{Z}/p\mathbb{Z})[x]$.
But since $s(x) \mid x^n - \overline{1}$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ we have a contradiction. The result now follows. □

Remark.

(1) ζ_n^j for $j = 1, \ldots, n$,$(j, n) = 1$ are the conjugates of ζ_n.
(2) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$
(3) $\mathbb{Q}(\zeta_n)$ is a normal extension of $\mathbb{Q}$ since $\zeta_n^i \in \mathbb{Q}(\zeta_n)$ for $\jmath = 1, \ldots, n$, $(j, n) = 1$.

---

8. Lecture: Friday, January 21, 2000

Theorem 17. *Let n be a positive integer. The Galois group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$.*

Proof:
The elements of the Galois group are the embeddings σ_k of $\mathbb{Q}(\zeta_n)$ in $\mathbb{C}$ defined by $\sigma_k(\zeta_n) = \zeta_n^k$ for $k = 1, \ldots, n$ with $(k, n) = 1$ and such that $\sigma_k(a) = a$ for all $a \in \mathbb{Q}$.
Let $\lambda : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ by $\lambda(\sigma_k) = k + n\mathbb{Z}$.
Certainly λ is a bijection. It remains then to show that λ is a group homomorphism:

$$\lambda(\sigma_k \circ \sigma_\ell) = \lambda(\sigma_{k\ell}) = k\ell + n\mathbb{Z} = (k + n\mathbb{Z})(\ell + n\mathbb{Z}) = \lambda(\sigma_k)\lambda(\sigma_\ell)$$

The result follows. □

Theorem 18. *Let n be a positive integer. If n is even, the only roots of unity in $\mathbb{Q}(\zeta_n)$ are the nth roots of unity. If n is odd, the only roots of unity in $\mathbb{Q}(\zeta_n)$ are the $2n$th roots of unity.*

Proof:
If n is odd, $\mathbb{Q}(\zeta_n) = \mathbb{Q}(-\zeta_n) = \mathbb{Q}(\zeta_{2n})$ and so it suffices to prove the result when n is even.
Let $\gamma = e^{2\pi i \frac{\ell}{s}}$ with ℓ and s coprime positive integers in $\mathbb{Q}(\zeta_n)$. There exist integers v and w such that

$$\gamma^v \zeta_n^w = e^{2\pi i(\frac{\ell v}{s} + \frac{w}{n})} = e^{2\pi i(\frac{\gcd(\ell n, s)}{sn})} = e^{2\pi i(\frac{\gcd(s,n)}{sn})} = e^{2\pi i(\frac{1}{lcm(s,n)})}$$

Let $b = \operatorname{lcm}(s, n)$ so that $\gamma^v \zeta_n^w = \mathbb{Q}(e^{\frac{2\pi i}{b}})$ has degree $\varphi(b)$ over $\mathbb{Q}$.
But we know that γ and ζ_n are in $\mathbb{Q}(\zeta_n)$, and so $\mathbb{Q}(e^{\frac{2\pi i}{b}})$ is contained in $\mathbb{Q}(\zeta_n)$, hence $\varphi(n) \geq \varphi(b)$. We have $b = \operatorname{lcm}(n, s)$.
Thus if $n = p_1^{h_1} \cdots p_r^{h_r}$ with $p_1, \ldots, p_r$ primes and $h_1, \ldots, h_r$ positive integers, then

$$b = p_1^{k_1} \cdots p_t^{k_t} \text{with } t \geq r \text{ and } k_i \geq h_i \text{ for } i = 1, \ldots, r.$$

Thus $\varphi(n) = (p_1^{h_1} - p_1^{h_1 - 1}) \cdots (p_r^{h_r} - p_r^{h_r - 1})$ while $\varphi(b) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_t^{h_t} - p_t^{h_t - 1})$.
But $\varphi(n) \geq \varphi(b)$. Note $\varphi(n) \mid \varphi(b)$. Thus $\varphi(n) = \varphi(b)$.
So n is even, we see that $n = b$. Thus, $n = \operatorname{lcm}(n, s)$ hence $s \mid n$. Thus φ is an nth root of unity. □

Definition. Let K be a finite extension of $\mathbb{Q}$. Say $[K : \mathbb{Q}] = n$. Let $\sigma_1, \ldots, \sigma_n$ denote the embedding of K is $\mathbb{C}$ which fix $\mathbb{Q}$.
For each $\alpha \in K$ we define the *trace* of α over K, denoted by $\mathrm{T}_{\mathbb{Q}}^K(\alpha)$, or when K and $\mathbb{Q}$ are understood denoted by $\mathrm{T}(\alpha)$, by

$$\mathrm{T}_{\mathbb{Q}}^K(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$$

and similarly we define the *norm* of α over K, denoted by $N_{\mathbb{Q}}^K(\alpha)$ (or $N(\alpha)$), by

$$N_{\mathbb{Q}}^K(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha)$$

Remark. Note that the trace is additive:

$$\mathrm{T}(\alpha + \beta) = \mathrm{T}(\alpha) + \mathrm{T}(\beta)$$

and the norm is multiplicative:

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

Further, if $r \in \mathbb{Q}$, and $\alpha \in K$, then $\mathrm{T}_{\mathbb{Q}}^K(r\alpha) = r\mathrm{T}_{\mathbb{Q}}^K(\alpha)$ and $N_{\mathbb{Q}}^K(r\alpha) = r^n N_{\mathbb{Q}}^K(\alpha)$

Theorem 19. *Let K be a finite extension of $\mathbb{Q}$, with $[K : \mathbb{Q}] = n$ and let $\alpha \in K$. Then $\mathrm{T}_{\mathbb{Q}}^K(\alpha) = \frac{n}{d}(\mathrm{T}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha))$ and $N_{\mathbb{Q}}^K(\alpha) = (N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha))^{\frac{n}{d}}$ where $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.*

Proof:
Each of the d embeddings of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ which fix $\mathbb{Q}$ extends to $[K : \mathbb{Q}(\alpha)] = \frac{n}{d}$ embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$ by Theorem 4. The result now follows from the definition of norm and trace. □

9. Lecture: Monday, January 24, 2000

Remark. Since the trace of α over $\mathbb{Q}(\alpha)$ and the norm of α over $\mathbb{Q}(\alpha)$ occur as coefficients in the minimal polynomial of α, they are rational numbers and are even rational integers if α is an algebraic integer.

Theorem 20. *Let K be a finite extension of $\mathbb{Q}$ and let $\alpha \in \mathbb{A} \cap K$.*

$$\alpha \text{ is a unit in } \mathbb{A} \cap K \Leftrightarrow N_{\mathbb{Q}}^{K}(\alpha) = \pm 1$$

(Here $\mathbb{A}$ denotes the ring of algebraic integers.)

Proof:
($\Rightarrow$): α is a unit in $\mathbb{A} \cap K$ implies that there is a β in $\mathbb{A} \cap K$ such that $\alpha\beta = 1$.
Thus $N_{\mathbb{Q}}^{K}(\alpha\beta) = N_{\mathbb{Q}}^{K}(1) = 1$.
Since the norm is multiplicative,

$$N_{\mathbb{Q}}^{K}(\alpha) N_{\mathbb{Q}}^{K}(\beta) = 1$$

But α and β are algebraic integers, hence $N_{\mathbb{Q}}^{K}(\alpha)$ and $N_{\mathbb{Q}}^{K}(\beta)$ are integers. Thus $N_{\mathbb{Q}}^{K}(\alpha) = \pm 1$.
($\Leftarrow$): Suppose $N_{\mathbb{Q}}^{K}(\alpha) = \pm 1$. Thus $N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = \pm 1$.
Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over $\mathbb{Q}$. Take

$$\pm\beta = \pm\alpha_2 \cdots \alpha_n = \frac{N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha)}{\alpha}$$

Then $\alpha\beta = 1$. □

Observe that by Theorem 20, we se that if K is some finite extension of $\mathbb{Q}$ with $K \subseteq \mathbb{C}$, then the units of $\mathbb{A} \cap K$ form a multiplicative subgroup of $\mathbb{C}^*$.
What are the units in $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$ where D is a squarefree integer? If $D \not\equiv 1 \pmod 4$, then $\mathbb{A} \cap \mathbb{Q}(\sqrt{D}) = \{\ell + m\sqrt{D} \mid \ell, m \in \mathbb{Z}\}$.
Thus if $\alpha = \ell + m\sqrt{D}$ is a unit in $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$, then

$$N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = (\ell + m\sqrt{D})(\ell - m\sqrt{D}) = \ell^2 - Dm^2 = \pm 1$$

Thus we look for solutions of the Diophantine equation $\ell - Dm^2 = \pm 1$ in integers ℓ and m.
Suppose that $D \equiv 1 \pmod 4$. Then

$$\mathbb{A} \cap \mathbb{Q}(\sqrt{D}) = \left\{ \frac{\ell + m\sqrt{D}}{2} \mid \ell, m \in \mathbb{Z}, \ell \equiv m \pmod 2 \right\}$$

Thus we search for solutions of $\ell^2 - Dm^2 = \pm 4$ with ℓ and m odd in addition to solutions of $\ell - Dm^2 = \pm 1$.

10. Lecture: Wednesday, January 26, 2000

Theorem 21. *Let D be a squarefree negative integer. The units in $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$ are ± 1 unless $D = -1$ in which case they are $\pm 1, \pm i$ or $D = -3$ in which case they are $\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}$.*

Proof:
If $D \not\equiv 1 \pmod 4$ then it suffices to look for solutions of the form $x^2 - Dy^2 = \pm 1$.
Since $D < 0$ we need only consider $x^2 - Dy^2 = 1$.

- If $D = -1$, we have the solutions $(x, y) = (\pm 1, 0) = (0, \pm 1)$ and the solutions correspond to the units $\pm 1, \pm i$.
- If $D < -1$, we see the only solutions are $(x, y) = (\pm 1, 0)$. Thus ± 1 are the only units in this case.

If $D \equiv 1 \pmod 4$, we must also consider the solutions of the equation $x^2 - Dy^2 = \pm 4$ in odd integers x and y hence, since $D < 0$, of $x^2 - Dy^2 = 4$.

- If $D = -3$, we have $x^2 + 3y^2 = 4$ and so the complete set of solutions is given by $(x, y) = (\pm 1, \pm 1)$. Thus the units in the ring of algebraic integers are $\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}$.
- If $D < -3$, then $x^2 - Dy^2 = 4$ has no solutions, with x and y odd and the result follows.

□

Suppose that D is a positive squarefree integer with $D > 1$. The unit group of $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$.
The units are formed by solving the equations $x^2 - Dy^2 = \pm 1$ and when $D = 1 \pmod 4$, $x^2 - Dy^2 = \pm 4$ in integers x and y. There is an algorithm for finding solutions called the continued fraction algorithm. It is based the following result. If $|N| < D$, then all solutions of $x^2 - dy^2 = N$ can be obtained as convergents from the continued fraction expansion of $\sqrt{D}$.

Theorem 22. *Let D be a squarefree integer with $D > 1$. There is a smallest unit larger than 1 in $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$. Let us denote it by ϵ. The unit group of $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$ is*

$$\{(-1)^k \epsilon^j \mid k \in \{0, 1\}, j \in \mathbb{Z}\}$$

Proof:
For the proof we'll appeal to the following result.

Lemma 23 (Dirichlet's Theorem)**.** *Let α be a real irrational number, and let $Q > 1$ be an integer. There exist integers p, q with $1 \leq q \leq Q$ such that $|q\alpha - p| < \frac{1}{Q}$.*
Further, there exist infinitely many pairs of integers (p, q) for which $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Proof:
Since α is irrational, and Q is at our disposal, the second assertion follows from the first.
We'll now prove the first assertion. For any real number x, let $\{x\}$ denote the fractional part of x, so $x = [x] + \{x\}$ where $[x]$ denotes the greatest integer less than or equal to x.
Consider the $Q + 1$ numbers $0, 1, \{\alpha\}, \ldots, \{(Q-1)\alpha\}$.
Notice that by the pigeonhole principle, there is an integer j with $1 \leq j \leq q$ such that two of the numbers are in the interval $[\frac{j-1}{Q}, \frac{j}{Q}]$. Thus, either there exist integers n, m with $n \neq m$, $1 \leq n \leq Q$ such that $|\{n\alpha\} - \{m\alpha\}| < \frac{1}{Q}$, or there exists an integer n with $1 \leq n \leq Q - 1$ and $t \in \{0, 1\}$ such that $|\{n\alpha\} - t| < \frac{1}{Q}$.

In the first case,

$$|(n\alpha - [n\alpha]) - (m\alpha - [m\alpha])| \leq \frac{1}{Q}$$
$$\Rightarrow |(n-m)\alpha - ([n\alpha] - [m\alpha])| \leq \frac{1}{Q}$$

Take $q = n - m$ and $p = [n\alpha] - [m\alpha]$ and the result follows since α is irrational and $Q > 1$ so strict inequality holds.
In the second case, $|n\alpha - [n\alpha] - t| \leq \frac{1}{Q}$, and so take $q = n$ and $p = [n\alpha] + t$. The result follows, as above. □

---

11. Lecture: Friday, January 28, 2000

We now continue with the proof of the theorem. We first show that there exists an integer m and infinitely many elements β of $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$ for which $N_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{D})}(\beta) = N(\beta) = m$.
Let $\theta = p + q\sqrt{D}$ with $p, q \in \mathbb{Z}, q > 0$.
Then $|N\theta| = \left|p + q\sqrt{D}\right| \left|p - q\sqrt{D}\right| = \left|\frac{p}{q} + \sqrt{D}\right| q^2 \left|\frac{p}{q} - \sqrt{D}\right|$.
By Dirichlet's Theorem, there exist infinitely many pairs (p, q) for which $q^2 \left|\frac{p}{q} - \sqrt{D}\right| < 1$.
For such p, q we have that $\left|\frac{p}{q} + \sqrt{D}\right| < 2\sqrt{D} + 1$. Thus there exist infinitely many $\theta \in \mathbb{A} \cap \mathbb{Q}(\sqrt{D})$ for which $|N\theta| \leq 2\sqrt{D}+1$. for which $N\theta = m$ for infinitely many $\theta \in \mathbb{A} \cap \mathbb{Q}(\sqrt{D})$.
Let $\theta_1 = p_1 + q_1\sqrt{D}$, $\theta_2 = p_2 + q_2\sqrt{D}$, and consider

$$N\left(\frac{\theta_1}{\theta_2}\right) = \frac{N(\theta_1)}{N(\theta_2)}$$

since the norm is multiplicative, and then $\frac{N(\theta_1)}{N(\theta_2)} = \frac{m}{m} = 1$. Further, we can find infinitely many θ's such that if θ_1 and θ_2 are in the set of θ's with $\theta_1 = p_1 + q_1\sqrt{D}$ and $\theta_2 = p_2 + q_2\sqrt{D}$ then $p_1 = p_2 \pmod{m}$ and $q_1 = q_2 \pmod{m}$.
Then let θ_2' be the conjugate of θ_2 over $\mathbb{Q}$ so that $N\theta_2 = \theta_2\theta_2' = m$. Observe that

$$\frac{\theta_1}{\theta_2} = 1 + \frac{\theta_1 - \theta_2}{\theta_2} = 1 + \left(\frac{\theta_1 - \theta_2}{\theta_2\theta_2'}\right)\theta_2' = 1 + \left(\left(\frac{p_1 - p_2}{m}\right) + \left(\frac{q_1 - q_2}{m}\right)\sqrt{D}\right)\theta_2' \in \mathbb{A} \cap \mathbb{Q}(\sqrt{D})$$

Since also $N(\frac{\theta_1}{\theta_2} = 1$, we see that $\frac{\theta_1}{\theta_2}$ is a unit in $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$. We next observe that if $|m| > 2$, then $\frac{\theta_1}{\theta_2} \neq 1$.
If $|m| \leq 2$, it is enough to consider a third θ, say θ_3, and then one of $\frac{\theta_1}{\theta_2}, \frac{\theta_2}{\theta_3}, \frac{\theta_1}{\theta_3}$ is different from -1.
Since ± 1 are the only roots of unity in $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$, we can find a unit in $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$ which is not a root of unity.
We consider the set $S = \{\gamma \in \mathbb{A} \cap \mathbb{Q}(\sqrt{D}) \mid \gamma > 0, \gamma \text{ a unit}\}$.
We have shown that S contains an element different from 1. Thus, on taking inverses if necessary, it contains an element strictly greater than 1.
To complete our proof, we'll show that $S = \{\epsilon^n \mid n \in \mathbb{Z}\}$ where ϵ is the smallest element of S larger than 1.

Let γ_0 be an element of $S, \gamma_0 > 1$. Then there are only finitely many elements β in S, $1 < \beta < \gamma_0$ since

$$\beta = \frac{p + q\sqrt{D}}{2}$$

for some $p.q \in \mathbb{Z}^+$.
Since $\beta > 1$, we see that p and q are not both negative. The conjugates of β are $\frac{p-q\sqrt{D}}{2} < \frac{p+q\sqrt{D}}{2}$. Therefore, both p and q are primitive.
Let ϵ be the smallest element of S which is strictly larger than 1. Suppose now that $\lambda \in S$ and λ is not of the form ϵ^n for any $n \in \mathbb{Z}$. Let n be such that $\epsilon^n < \lambda < \epsilon^{n+1}$.
Then $\frac{\lambda}{\epsilon^n}$ is in S and we get $1 < \frac{\lambda}{\epsilon^n} < \epsilon$. This contradicts the minimality of ϵ and the result follows. □

Definition. Let $K \subseteq L \subseteq \mathbb{C}$ with L a finite extension of K, say $[L : K] = n$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of L in $\mathbb{C}$ which fix K. Let $\alpha \in L$, then the trace of α from L to K, denoted $T_K^L(\alpha)$, is given by

$$T_K^L(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$$

The the norm from L to K of α, denoted by $N_K^L(\alpha)$, is given by

$$N_K^L(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha)$$

12. Lecture: Monday, January 31, 2000

Theorem 24. *Let $K, L,$, and M be finite extensions of $\mathbb{Q}$ with $K \subseteq L \subseteq M$. Then, for all $\alpha \in M$,*

$$T_K^M(\alpha) = T_K^L(T_L^M(\alpha))$$

and

$$N_K^M(\alpha) = N_K^L(N_L^M(\alpha))$$

Proof:
We'll prove the result for trace only (the norm works similarly).
Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of L in $\mathbb{C}$ which fix K. Let $\tau_1, \ldots, \tau_m$ be the embeddings of M in $\mathbb{C}$ which fix L.
Let N be a normal extension of $\mathbb{Q}$ which contains M. Each map σ_i and τ_i can be extended to an automorphism of N.
Let $\sigma_1', \ldots, \sigma_n', \tau_1', \ldots, \tau_m'$ be some choice of extensions of $\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m$ respectively to automorphisms of N. Then

$$T_K^L(T_L^M(\alpha)) = \sum_{i=1}^{n} \sigma_i(\sum_{j=1}^{m} \tau_j(\alpha)) = \sum_{i=1}^{n} \sigma_i'(\sum_{j=1}^{m} \tau_j'(\alpha)) = \sum_{\substack{1\le i\le n\\ 1\le j\le m}}^{n} \sigma_i'\tau_j'(\alpha)$$

It remains to show that the nm embeddings of M in $\mathbb{C}$ which fix K are given by $\sigma_i'\tau_{j|M}'$ (where $|M$ indicates the restriction to M) for $i = 1, \ldots, n$, $j = 1, \ldots, m$. Since there are nm such embeddings, it suffices to show that they are distinct.
Suppose $\sigma_i'\tau_{j|M}' = \sigma_r'\tau_{s|M}'$. Next let α be such that $L = K[\alpha]$.
Then $\sigma_i(\alpha) = \sigma_i'(\alpha) = \sigma_i'(\tau_j'(\alpha)) = \sigma_i'\tau_{j|M}'(\alpha) = \sigma_r'\tau_{s|M}'(\alpha) = \sigma_r'\tau_s'(\alpha) = \sigma_r'(\tau_s'(\alpha)) = \sigma_r'(\alpha) = \sigma_r(\alpha)$.
So since the behaviour of σ_i is completely determined by its action of α, we conclude that $\sigma_i = \sigma_r \implies r = i$.
Next choose β so that $M = L[\beta]$. Then since $\sigma_i'\tau_{j|M}(\beta) = \sigma_i'\tau_{s|M}(\beta)$ we see that $\tau_j(\beta) = \tau_s(\beta)$. Thus since the embeddings of M in $\mathbb{C}$ which fix L are determined by their effect on β we see that $\tau_j = \tau_s$ hence $j = s$. Then we have that $\sigma_i'\tau_{j|M}'$, $i = 1, \ldots, n$, $1, \ldots, m$ are all distinct and the result follows. □

Definition. Let K be an extension of $\mathbb{Q}$ of degree n and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$. For any set $\{\alpha_1, \ldots, \alpha_n\}$ of of elements of K, we define the *discriminant of* $\{\alpha_1, \ldots, \alpha_n\}$, denoted by $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$, as $(\det(\sigma_i(\alpha_k))^2$.

Note that the order in which we take $\alpha_1, \ldots, \alpha_n$ or the order in which we take the embeddings $\sigma_1, \ldots, \sigma_n$ does not matter and so the discriminant is well-defined.

Theorem 25. *Let K be an extension of $\mathbb{Q}$ of degree n. Let $\alpha_1, \ldots, \alpha_n$ be in K. Then*

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(T_{\mathbb{Q}}^K(\alpha_i\alpha_j))$$

Proof:
Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$. Then

$$(\sigma_j(\alpha_i))(\sigma_i(\alpha_j)) = (\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j)) = T^J_{\mathbb{Q}}(\alpha_i\alpha_j)$$

But $\text{disc}(\alpha_1, \ldots, \alpha_n) = (\det(\sigma_i(\alpha_j)))^2 = \det(\sigma_j(\alpha_i))\det(\sigma_i(\alpha_j)) = \det((\sigma_j(\alpha_i))(\sigma_i(\alpha_j))) = \det(T^K_{\mathbb{Q}}(\alpha_i\alpha_j))$ □

---

13. Lecture: Wednesday, February 2, 2000

Corollary 26. *Let K be an extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] = n$. Let $\alpha_1, \ldots, \alpha_n$ be elements of K. Then $\text{disc}(\alpha_1, \ldots, \alpha_n)$ is a rational number and if $\alpha_1, \ldots, \alpha_n$ are algebraic integers, then $\text{disc}(\alpha_1, \ldots, \alpha_n)$ is a rational integer.*

Proof:
Since $T^K_{\mathbb{Q}}(\alpha_i\alpha_j) \in \mathbb{Q}$ for $1 \le i \le n$, $1 \le j \le n$ the first claim follows immediately from Theorem 25.
Since the sum and product of two algebraic integers is an algebraic integer, then $T^K_{\mathbb{Q}}(\alpha_i\alpha_j)$ is an algebraic integer and hence a rational integer. The result again follows from Theorem 25. □

Let $[K : \mathbb{Q}] = n$. Assume that $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ are bases for K as a vector space over $\mathbb{Q}$. Then

$$\beta_k = \sum_{j=1}^{n} c_{k,j}\alpha_j \text{ for } k = 1, \ldots, n$$

where the $c_{k,j}$'s are in $\mathbb{Q}$. Thus

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & & \vdots \\ c_{n,1} & \cdots & c_{n,n} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$. We have $\sigma_i(\beta_k) = \sum_{j=1}^{n} c_{k,j}\sigma_i(\alpha_k)$ for $i = 1, \ldots, n$ and $k = 1, \ldots, n$. Therefore,

$$\begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \vdots & & \vdots \\ \sigma_1(\beta_n) & \cdots & \sigma_n(\beta_n) \end{pmatrix} = \begin{pmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & & \vdots \\ c_{n,1} & \cdots & c_{n,n} \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$$

Then

$$\text{disc}(\beta_1, \ldots, \beta_n) = (\det(c_{i,j}))^2 \text{disc}(\alpha_1, \ldots, \alpha_n) \tag{1}$$

Let $K = \mathbb{Q}(\theta)$. Then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis for K over $\mathbb{Q}$. Notice that $\text{disc}(1, \theta, \ldots, \theta^{n-1}) =$

$$(\det \begin{pmatrix} \sigma_1(1) & \sigma_1(\theta) & \cdots & \sigma_1(\theta^{n-1}) \\ \vdots & & & \vdots \\ \sigma_n(1) & \sigma_n(\theta) & \cdots & \sigma_n(\theta^{n-1}) \end{pmatrix})^2 = (\det \begin{pmatrix} 1 & \sigma_1(\theta) & \cdots & (\sigma_1(\theta))^{n-1} \\ \vdots & & & \vdots \\ 1 & \sigma_n(\theta) & \cdots & (\sigma_n(\theta))^{n-1} \end{pmatrix})^2$$

Since this is a van der Monde determinant, then $\text{disc}(1,\theta,\dots,\theta^{n-1}) = (\prod_{i<j}(\sigma_i(\theta)-\sigma_j(\theta)))^2$.
Notice that $\sigma_1(\theta),\dots,\sigma_n(\theta)$ are the conjugates of θ over $\mathbb{Q}$, and so are distinct. Thus, in particular, $\text{disc}(1,\theta,\dots,\theta^{n-1}) \neq 0$.
If $(\alpha_1,\dots,\alpha_n)$ is a basis for K over $\mathbb{Q}$ and we take $\{\beta_1,\dots,\beta_n\}$ to be $\{1,\theta,\dots,\theta^{n-1}\}$ we see from (1) that $\text{disc}(1,\theta,\dots,\theta^{n-1}) \neq 0$ and $\det(c_{i,j}) \neq 0$.
We conclude that the discriminant of any basis for K over $\mathbb{Q}$ is nonzero.

Remark. If $K \subseteq \mathbb{R}$, then by (1), the determinant of any basis for K over $\mathbb{Q}$ is positive since plainly $\text{disc}(1,\theta,\dots,\theta^{n-1})$ is positive.

Theorem 27. *Let $[K:\mathbb{Q}] = n$, and let $\alpha_1,\dots,\alpha_n$ be in K. We have $\text{disc}(1,\theta,\dots,\theta^{n-1}) = 0$ iff $\alpha_1,\dots,\alpha_n$ are linearly dependent over $\mathbb{Q}$.*

Proof:
($\Leftarrow$): Since $\alpha_1,\dots,\alpha_n$ are linearly dependent over $\mathbb{Q}$, the columns of $(\sigma_i(\alpha_j))$ are linearly dependent over $\mathbb{Q}$. Thus the determinant of the matrix if 0, hence $\text{disc}(1,\theta,\dots,\theta^{n-1}) = 0$.
($\Rightarrow$): If $\text{disc}(1,\theta,\dots,\theta^{n-1}) = 0$, then by (1), $\alpha_1,\dots,\alpha_n$ is not a basis for K over $\mathbb{Q}$ and thus $\{\alpha_1,\dots,\alpha_n\}$ is not a linearly independent set. □

The following observation is useful for computing $\text{disc}(1,\theta,\dots,\theta^{n-1})$ where $K = \mathbb{Q}(\theta)$ and $[K:\mathbb{Q}] = n$. We have

$$\text{disc}(1,\theta,\dots,\theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^K(f'(\theta))$$

where f is the minimal polynomial for θ over $\mathbb{Q}$.
Let $\theta = \theta_1,\dots,\theta_n$ be the conjugates of θ over $\mathbb{Q}$. We have

$$\text{disc}(1,\theta,\dots,\theta^{n-1}) = \prod_{1\le i<j\le n}(\theta_i-\theta_j)^2$$

We have $f(x) = (x-\theta_1)\cdots(x-\theta_n)$ and so

$$f'(x) = \sum_{j=1}^{n}\prod_{i=1,i\neq j}^{n}(x-\theta_i) \implies N_{\mathbb{Q}}^K(f'(\theta)) = \prod_{k=1}^{n} f'(\theta_k) = \prod_{k=1}^{n}(\prod_{i=1,i\neq j}^{n}(\theta_k-\theta_i))$$

Note that $(\theta_i-\theta_j)(\theta_j-\theta_i) = -(\theta_i-\theta_j)^2$. Thus

$$\prod_{1\le i<j\le n}(\theta_i-\theta_j)^2 = (-1)^{\frac{n(n-1)}{2}}\prod_{k=1}^{n}(\prod_{i=1,i\neq j}^{n}(\theta_k-\theta_i))$$

and the result follows.

Let K be a finite extension of $\mathbb{Q}$ and let $\theta \in K$. Suppose $[K:\mathbb{Q}] = n$. Then we abbreviate $\text{disc}(1,\theta,\dots,\theta^{n-1})$ by $\text{disc}(\theta)$.

Theorem 28. *Let n be a positive integer and let $\zeta_n = e^{2\pi i/n}$. Then in $\mathbb{Q}(\zeta_n)$, $\text{disc}(\zeta_n)$ divides $n^{\varphi(n)}$. Further, if p is an odd prime, $\text{disc}(\zeta_p) = (-1)^{\frac{p(p-1)}{2}}p^{p-2}$.*

Proof:
Let $\Phi_n(x)$ be the nth cyclotomic polynomial. $\Phi_n(x)$ is the minimal polynomial of ζ_n. Thus $x^n - 1 = \Phi_n(x)g(x)$ where $g \in \mathbb{Z}[x]$.
Note that $nx^{n-1} = \Phi_n(x)g'(x) + {\Phi_n}'(x)g(x)$. Thus $n{\zeta_n}^{n-1} = {\Phi_n}'(\zeta_n)g(\zeta_n)$. $(*)$
And so $N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(n)N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(\zeta_n^{n-1}) = N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(\Phi_n'(\zeta_n))N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(g(\zeta_n))$.
Thus $n^{\varphi(n)} = \pm\text{disc}(1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1})N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(g(\zeta_n))$.
Since $g \in \mathbb{Z}[x]$ and ζ_n is an algebraic integer, $g(\zeta_n)$ is an algebraic integer, and so $N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(g(\zeta_n))$ is an integer. Thus $\text{disc}(\zeta_n) \mid n^{\varphi(n)}$.
Let p be an odd prime. Then

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1}$$

and $g(x) = x - 1$. Thus by $(*)$,

$$p = \zeta_p \Phi_p'(\zeta_p) g(\zeta_p)$$

hence

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(p) = N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\zeta_p) N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\Phi_p'(\zeta_p)) N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\zeta_p - 1) \tag{1}$$

But,

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\zeta_p) = e^{(\frac{2\pi i}{p})\frac{p(p-1)}{2}} = 1 \text{ since } p \text{ is an odd prime} \tag{2}$$

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\Phi_p'(\zeta_p)) = (-1)^{\frac{p(p-1)}{2}}\text{disc}(\zeta_p) \text{ since } p \text{ is an odd prime} \tag{3}$$

Further,

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\zeta_p - 1) = \prod_{j=1}^{p-1}(\zeta_p^j - 1) = \prod_{j=1}^{p-1}(1 - \zeta_p^j) = \Phi_p(1) \tag{4}$$

and

$$\Phi_p(1) = \overbrace{1 + \cdots + 1}^{p \text{ times}} = p \tag{5}$$

Finally, we observe that

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(p) = p^{p-1} \tag{6}$$

The result follows from (1) through (6). □

Definition. Let K be a finite extension of $\mathbb{Q}$. A set of algebraic integers $\{\alpha_1, \ldots, \alpha_s\}$ is said to be an *integral basis* for K if every γ in $\mathbb{A} \cap K$ has a unique representation of the form $\gamma = m_1\alpha_1 + \cdots + m_s\alpha_s$ with $m_1, \ldots, m_s$ rational integers.
Note that an integral basis for K (over $\mathbb{Q}$) is a basis for K over $\mathbb{Q}$.
Note: $\text{span}\{\alpha_1, \ldots, \alpha_s\} = K$ since if $\theta \in K$, there exists a nonzero integer r such that $r\theta \in \mathbb{A} \cap K$ for which $r\theta = m_1\alpha_1 + \cdots + m_s\alpha_s$ and so $\theta = \frac{m_1}{r}\alpha_1 + \cdots + \frac{m_s}{r}\alpha_s$.
Thus $\text{span}\{\alpha_1, \ldots, \alpha_s\} = K$.

Note: $\{\alpha_1, \ldots, \alpha_s\}$ are linearly independent over $\mathbb{Q}$ since otherwise there exist rationals $t_1, \ldots, t_s$ not all zero such that

$$t_1\alpha_1 + \cdots + t_s\alpha_s = 0$$

Clearing denominators we obtain a nontrivial integer linear combination of $\alpha_1, \ldots, \alpha_s$ which is zero. We also have the trivial linear combination and this contradicts the uniqueness of representation for an integral basis.

14. Lecture: Monday, February 7, 2000

Theorem 29. *Let K be a finite extension of $\mathbb{Q}$. Then K has an integral basis.*

Proof:
Let θ be an algebraic integer such that $K = \mathbb{Q}(\theta)$. Consider the set of all bases for K over $\mathbb{Q}$ (as a vector space) whose elements are algebraic integers.
The set is nonempty since it contains the basis $\{1, \theta, \dots, \theta^{n-1}\}$ where $n = [K : \mathbb{Q}]$.
The discriminants of the bases in the set are integers since the bases consist of algebraic integers. Thus the absolute values of the discriminants are positive integers. Note that they are nonzero, since the discriminant of the basis is nonzero.
Choose a basis $\omega_1, \dots, \omega_n$ for which $|\text{disc}(\omega_1, \dots, \omega_n)|$ is minimal. We'll verify that $\{\omega_1, \dots, \omega_n\}$ is an integral basis.
Suppose that $\{\omega_1, \dots, \omega_n\}$ is not an integral basis. Then there is a $\gamma \in \mathbb{A} \cap K$ for which $\gamma = a_1\omega_1 + \cdots + a_n\omega_n$, but with not all the $a_i's$ in $\mathbb{Z}$. So without loss of generality, suppose that a_1 is not an integer.
Then $a_1 = a + r$ with $a \in \mathbb{Z}$ and $0 < r < 1$. Notice that ${\omega_1}^*, \dots, {\omega_n}^*$ is a basis for K over $\mathbb{Q}$ consisting of algebraic integers if we put ${\omega_1}^* = \gamma - a\omega_1$ and ${\omega_i}^* = \omega_i$ for $i = 2, \dots, n$. So

$$\text{disc}({\omega_1}^*, \dots, {\omega_n}^*) = \left(\det \begin{pmatrix} a_1 - a & a_2 & \cdots & a_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \right) \text{disc}(\omega_1, \dots, \omega_n)$$

$$= (a_1 - a)^2 \text{disc}(\omega_1, \dots, \omega_n) = r^2 \text{disc}(\omega_1, \dots, \omega_n)$$

Thus $|\text{disc}({\omega_1}^*, \dots, {\omega_n}^*)| = r^2 \, |\text{disc}(\omega_1, \dots, \omega_n)| < |\text{disc}(\omega_1, \dots, \omega_n)|$ and this contradiction completes the proof. □

Theorem 30. *Let K be a finite extension of $\mathbb{Q}$. All integral bases for K over $\mathbb{Q}$ have the same discriminant.*

Proof:
Let $\{\alpha_1, \dots, \alpha_n\}$, $\{\beta_1, \dots, \beta_n\}$ be two integral bases for K. Then

$$\alpha_j = \sum_{i=1}^{n} c_{ij}\beta_i \text{ for some } c_{ij} \in \mathbb{Z}$$

Thus $\text{disc}(\alpha_1, \dots, \alpha_n) = (\det(c_{ij}))^2 \text{disc}(\beta, \dots, \beta_n)$.
Since $c_{ij} \in \mathbb{Z}$ for $i = 1, \dots, n$, $j = 1, \dots, n$ we see that $\det(c_{ij}) \in \mathbb{Z}$.
Thus $\text{disc}(\beta, \dots, \beta_n) \mid \text{disc}(\alpha_1, \dots, \alpha_n)$.
Similarly we see that $\text{disc}(\alpha_1, \dots, \alpha_n) \mid \text{disc}(\beta, \dots, \beta_n)$.
Thus $\text{disc}(\alpha_1, \dots, \alpha_n) = \pm\text{disc}(\beta, \dots, \beta_n)$. Since $(\det(c_{ij}))^2 > 0$, then we see that the two discriminants are equal. □

Definition. Let K be a finite extension of $\mathbb{Q}$. The *discriminant of K* is the discriminant of an integral basis for K.

Remark. For any finite extension K of $\mathbb{Q}$, the discriminant d of K is an integer with $|d| \geq 1$.
It can be shown that if $K \neq \mathbb{Q}$, then $|d| > 1$.

Let D be a squarefree integer with $|D| \neq 1$. What is the discriminant of $\mathbb{Q}(\sqrt{D})$?
If $D \not\equiv 1 \pmod 4$, then $\{1, \sqrt{D}\}$ forms an integral basis for $\mathbb{Q}(\sqrt{D})$. Further,

$$\operatorname{disc}(1, \sqrt{D}) = (\det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix})^2 = 4D$$

If $D \equiv 1 \pmod 4$, then the algebraic integers in $\mathbb{Q}(\sqrt{D})$ are of the form $\frac{\ell + m\sqrt{D}}{2}$ with $\ell, m \in \mathbb{Z}$ and $\ell \equiv m \pmod 2$.
Then $\{1, \frac{1+\sqrt{D}}{2}\}$ forms an integral basis for $\mathbb{Q}(\sqrt{D})$. We have

$$\operatorname{disc}(1, \tfrac{1+\sqrt{D}}{2}) = \left(\det \begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix}\right)^2 = (-\sqrt{D})^2 = D$$

We will now prove that for each positive integer $n \in \mathbb{Z}^+$, $\mathbb{A} \cap \mathbb{Q}(\zeta_n) = \mathbb{Z}[\zeta_n]$. In particular, $\{1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}\}$ is an integral basis for $\mathbb{Q}(\zeta_n)$.
Notice that, as a consequence of Theorem 28, we then have, for p an odd prime, that the discriminant of $\mathbb{Q}(\zeta_p)$ is $(-1)^{\frac{p-1}{2}} p^{(}p-2)$.

---

15. Lecture: Wednesday, February 9, 2000

Theorem 31. *Let K be a finite extension of $\mathbb{Q}$, and let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for K over $\mathbb{Q}$. Let $d = \operatorname{disc}\{\alpha_1, \ldots, \alpha_n\}$. If $\alpha \in \mathbb{A} \cap K$, there exist $m_1, \ldots, m_n \in \mathbb{Z}$ such that $d \mid m_i^2$ for $i = 1, \ldots, n$ and $\alpha = \frac{m_1\alpha_1 + \ldots + m_n\alpha_n}{d}$.*

Proof:
Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$. Write $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ with $a_i \in \mathbb{Q}$, for $i = 1, \ldots, n$. Then $\sigma_j(\alpha) = a_1\sigma_j(\alpha_1) + \cdots + a_n\sigma_j(\alpha_n)$ for $j = 1, \ldots, n$. Thus

$$\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}$$

By Cramer's Rule,

$$a_j = \frac{\det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha) & \cdots & \sigma_n(\alpha_1) \\ \vdots & & & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_1(\alpha) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}}{\det(\sigma_i(\alpha_j))}$$

Thus $a_j = \frac{\gamma_j}{\delta}$, where $\gamma_1, \ldots, \gamma_n$ and δ are algebraic integers and $\delta^2 = d(= \operatorname{disc}(\alpha_1, \ldots, \alpha_n))$. Therefore, $da_j = \delta\gamma_j$. Note that $da_j \in \mathbb{Q}$ and $\delta\gamma_j$ is an algebraic integer. Thus da_j is an integer. Put $m_j = da_j$ for $j = 1, \ldots, n$.

It remains to show that $d \mid {m_j}^2$ for $j = 1, \ldots, n$. But $\frac{{m_j}^2}{d} = da_j^2 = d\left(\frac{\gamma_j}{\delta}\right)^2 = {\gamma_j}^2$ for

$j = 1, \ldots, n$.
Thus $\frac{{m_j}^2}{d} \in \mathbb{Q}$ and is an algebraic integer, so $\frac{{m_j}^2}{d}$ is an integer. Thus $d \mid {w_j}^2$ for $j = 1, \ldots, n$. □

Let K be a finite extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] = n$. Let θ be such that $K = \mathbb{Q}(\theta)$. The embeddings of K in $\mathbb{C}$ are determined once we know the image of θ under the embeddings. θ must be sent to once of its conjugates.
Let $\theta = \theta_1, \ldots, \theta_n$ be the conjugates of θ. For each $i = 1, \ldots, n$ we have that $\overline{\theta_i}$ is also a conjugate of θ. This follows from that fact the $\theta_1, \ldots, \theta_n$ are the roots of the minimal polynomial f of θ over $\mathbb{Q}$ and $f \in \mathbb{R}[x]$.
Thus the embeddings of K in $\mathbb{C}$ which do not map K into $\mathbb{R}$ come in pairs. These are known as the *complex embeddings* and the balance are known as the *real embeddings*. Thus

$$n = r_1 + 2r_2$$

where r_1 is the number of real embeddings, and $2r_2$ is the number of complex embeddings. If σ is a complex embedding, then it has the embedding $\overline{\sigma}$ associated with it.

Proposition 32. *Let K be a finite extension of $\mathbb{Q}$ with exactly $2r_2$ complex embeddings. The sign of the determinant of K is $(-1)^{r_2}$.*

Proof:
Let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis for K. Then $\operatorname{disc}(K) = (\det(\sigma_i(\alpha_j)_{\substack{i=1,\ldots,n \\ j=1,\ldots,n}}))^2$
Notice that $\det(\sigma_i(\alpha_j))^2 = \begin{pmatrix} \overline{\sigma_1(\alpha_1)} & \cdots & \overline{\sigma_1(\alpha_n)} \\ \vdots & & \vdots \\ \overline{\sigma_n(\alpha_1)} & \cdots & \overline{\sigma_n(\alpha_n)} \end{pmatrix} = (-1)^{r_2} \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$
since complex conjugation induces r_2 row exchanges. Note that if r_2 is even that $\det(\sigma_i(\alpha_j))$ is real and if r_2 is odd it is purely imaginary. The result follows on squaring the number. □

We now return to proving that $\mathbb{Z}[\zeta_n]$ is $\mathbb{A} \cap \mathbb{Q}(\zeta_n)$ for $n = 1, \ldots$. We'll prove that initially for the case when $n = p^r$ with p a prime and $r \in \mathbb{Z}^+$.
Note that

$$\Phi_{p^r}(x) = \prod_{\substack{j=1 \\ (j,p)=1}}^{p^r} (x - (\zeta_{p^r})^j) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = 1 + x + x^{p^{r-1}} + \cdots + x^{(p-1)p^{r-1}}$$

In particular, $\Phi_{p^r}(1) = p$.

---

16. Lecture: Friday February 11, 2000

Theorem 33. *Let p be a prime number and r a positive integer. The ring of algebraic integers of $\mathbb{Q}(\zeta_{p^r})$ is $\mathbb{Z}[\zeta_{p^r}]$. (Here $\zeta_n = e^{2\pi i/n}$ for $n = 1, 2, \ldots$).*

Proof:
We have $\mathbb{Q}(\zeta_{p^r}) = \mathbb{Q}(1 - \zeta_{p^r})$ and $\{1, (1 - \zeta_{p^r}), \ldots, (1 - \zeta_{p^r})^s\}$ is a basis for $\mathbb{Q}(\zeta_{p^r})$ over $\mathbb{Q}$, where $s = \varphi(p^r)$.

By Theorem 31, if $\alpha \in \mathbb{A} \cap \mathbb{Q}(\zeta_{p^r})$, then

$$\alpha = \frac{m_1 + m_2(1-\zeta_{p^r}) + \cdots + m_s(1-\zeta_{p^r})^{s-1}}{d} \qquad (*)$$

where $d = \text{disc}(1-\zeta_{p^r})$. Note that

$$d = \prod_{\substack{1\le i\le j\le p^r \\ (i,p)=1,(j,p)=1}} ((1-(\zeta_{p^r})^i) - (1-(\zeta_{p^r})^j))^2 = \prod_{\substack{1\le i\le j\le p^r \\ (i,p)=1,(j,p)=1}} ((\zeta_{p^r}^i) - (\zeta_{p^r}^j))^2 = \text{disc}(\zeta_{p^r})$$

By Theorem 28, $\text{disc}(\zeta_{p^r})$ is a power of p. Suppose that $\mathbb{A}\cap\mathbb{Q}(\zeta_{p^r}) \neq \mathbb{Z}[\zeta_{p^r}]$. Then $\mathbb{A}\cap\mathbb{Q}(\zeta_{p^r}) \neq \mathbb{Z}[1-\zeta_{p^r}]$.
Then by $(*)$ and by the fact that $\text{disc}(\zeta_{p^r})$ is a power of p, we see that there is an $\alpha \in \mathbb{A}\cap\mathbb{Q}(\zeta_{p^r})$ such that

$$\alpha = \frac{\ell_1 + \ell_2(1-\zeta_{p^r}) + \cdots + \ell_s(1-\zeta_{p^r})^{s-1}}{d}$$

where $\ell_1, \ldots, \ell_s$ are integers, not all of which are divisible by p.
Let i be the smallest positive integer for which $p \nmid \ell_i$. Then

$$\gamma = \frac{\ell_i(1-\zeta_{p^r})^{i-1} + \cdots + \ell_s(1-\zeta_{p^r})^{s-1}}{p}$$

is an algebraic integer.
(Recall that $p = \Phi_{p^r}(1) = \prod_{\substack{j=1 \\ (j,p)=1}}^{p^r} (1-\zeta_{p^r}^j)$).
Since $1-x$ divides $1-x^k$ in $\mathbb{Z}[x]$ for $k = 1, \ldots$ we see that $p = (1-\zeta_{p^r})^s\lambda$ where $\lambda \in \mathbb{A}\cap\mathbb{Q}(\zeta_{p^r})$.
Therefore, $(1-\zeta_{p^r})^{s-i}\lambda\gamma \in \mathbb{A} \cap \mathbb{Q}(\zeta_{p^r})$ and so

$$(1-\zeta_{p^r})^{s-i}\lambda\gamma = \frac{\gamma\ell_i(1-\zeta_{p^r})^{i-1} + \cdots + \ell_s(1-\zeta_{p^r})^s}{(1-\zeta_{p^r})^i}$$

We conclude that $\theta = \frac{\ell_i}{1-\zeta_{p^r}}$ is an algebraic integer. Thus $(1-\zeta_{p^r})\theta = \ell_i$ and so

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{p^r})}(\theta) N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{p^r})}(1-\zeta_{p^r}) = N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{p^r})}(\ell_i)$$

Since θ is an algebraic integer, then $N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{p^r})}(\theta)$ is an integer, and thus $N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{p^r})}(1-\zeta_{p^r})$ divides ${\ell_i}^s$. But $N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{p^r})}(1-\zeta_{p^r}) = p$ and this is a contradiction since $p \nmid \ell_i$. □

Next stage: to pass from $n = p^r$ to a general positive integer n.

Definition. Let L be finite extensions of $\mathbb{Q}$. The *compositum* of L and K, denoted LK, is the smallest field containing $L \cup K$.
What is the connection between $\mathbb{A} \cap K$, $\mathbb{A} \cap L$, and $\mathbb{A} \cap LK$?

Lemma 34. *Let L and K be finite extensions of $\mathbb{Q}$, with $[K:\mathbb{Q}] = m$ and $[L:\mathbb{Q}] = n$. Suppose that the degree of the compositum is maximal. Suppose that $[LK:\mathbb{Q}] = mn$.*
Let σ be an embedding of K in $\mathbb{C}$, and let τ be an embedding of L in $\mathbb{C}$.
Then there is an embedding of LK in $\mathbb{C}$ which restricts to σ on K and τ on L.

Proof:
σ has n distinct extensions to embeddings LK in $\mathbb{C}$, since $[LK : K] = n$; recall $[LK : \mathbb{Q}] = mn$ and $[K : \mathbb{Q}] = m$.
Each of the embeddings is distinct when restricted to L. We obtain in this way mn embeddings of LK in $\mathbb{C}$. Since $[LK : \mathbb{Q}] = mn$, this is all of them.
Thus one of them, restricted to L, is τ. $\square$

17. Lecture: Monday, February 14, 2000

Theorem 35. *Let K and L be finite extensions of $\mathbb{Q}$ of degree m and n respectively. Let R, S, and T denote $\mathbb{A} \cap K$, $\mathbb{A} \cap L$, and $\mathbb{A} \cap KL$ respectively. Suppose $[KL : \mathbb{Q}] = mn$. Let $d = \gcd(\mathrm{disc}(R), \mathrm{disc}(S))$. Then*

$$T \subseteq \frac{1}{d} RS$$

Proof:
Let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis for K and let $\{\beta_1, \ldots, \beta_m\}$ be an integral basis for L. $KL = \mathrm{span}\{\alpha_1\beta_1, \ldots, \alpha_n\beta_m\}$. Since $[KL : \mathbb{Q}] = mn$, we see $\{\alpha_1\beta_1, \ldots, \alpha_n\beta_m\}$ is a basis for KL over $\mathbb{Q}$.
Thus every α in KL has a representation of the form

$$\alpha = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{a_{ij}\alpha_i\beta_j}{r}$$

where a_{ij} for $i = 1, \ldots, m$, $j = 1, \ldots, n$ and r are integers with

$$\gcd(a_{11}, \ldots, a_{mn}, r) = 1$$

To prove the theorem it suffices to show that $r \mid d$. By symmetry it suffices to show that $r \mid \mathrm{disc}(R)$.
By Lemma 34 every embedding σ of K in $\mathbb{C}$ can be extended to an embedding σ' of KL in $\mathbb{C}$ which fixes each element of L. Thus

$$\sigma'(\alpha) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \frac{a_{ij}\alpha_i\beta_j}{r} \right) \sigma(\alpha_i)$$

Put $x_i = \displaystyle\sum_{j=1}^{n} \frac{a_{ij}\beta_j}{r}$ for $i = 1, \ldots, m$.

Thus $\sigma'(\alpha) = \displaystyle\sum_{i=1}^{m} \sigma(\alpha_i) x_i$.

Therefore

$$\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_m) \\ \vdots & \ddots & \cdots \\ \sigma_m(\alpha_1) & \cdots & \sigma_m(\alpha_m) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} \sigma'(\alpha) \\ \vdots \\ \sigma'(\alpha) \end{pmatrix}$$

We now solve for the x_i's using Cramer's rule:

$$x_i = \frac{\det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_i) & \cdots & \sigma_1(\alpha_m) \\ \vdots & & & & \cdots \\ \sigma_m(\alpha_1) & \cdots & \sigma_m(\alpha_i) & \cdots & \sigma_m(\alpha_m) \end{pmatrix}}{\det(\sigma_i(\alpha_j))}$$

Thus $x_i = \frac{\gamma_i}{\delta}$ where $\lambda_i \in \mathbb{A}$ and $\delta^2 \in \text{disc}(R)$. Accordingly $\text{disc}(R)x_i = \delta\gamma_i$ and $\delta\gamma_i$ is an algebraic integer. But $\text{disc}(R)x_i \in \mathbb{Q}$ hence in $\mathbb{Z}$.
Thus

$$\text{disc}(R)x_i = \sum_{j=1}^{n} \left(\frac{\text{disc}(R)a_{ij}}{r} \right) \beta_j \text{ for } i = 1, \ldots, m.$$

Since $\text{disc}(R)x_i$ is an integer and so is in S and since $\{\beta_1, \ldots, \beta_n\}$ is an integral basis for L, we see that $\dfrac{\text{disc}(R)a_{ij}}{r}$ is an integer for $i = 1, \ldots, m$, $j = 1, \ldots, n$. Finally since $\gcd(r, a_{11}, \ldots, a_{mn}) = 1$ we see that $r \mid \text{disc}(R)$ as required. □

Theorem 36. *Let n be a positive integer. The ring of algebraic integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}(\zeta_n)$.*

Proof:
We'll prove by induction on r, the number of distinct prime factors of n.
If $r = 1$, the result follows from Theorem 33. Suppose the result holds for $q \leq r \leq k$.
Let $n = p_1^{\ell_1} \cdots p_k^{\ell_k}$ where $\ell_1, \ldots, \ell_k$ are positive integers and $p_1, \ldots, p_k$ are distinct primes.
By inductive hypothesis,

$$A \cap \mathbb{Q}(\zeta_{{p_1}^{\ell_1} \cdots {p_{k-1}}^{\ell_{k-1}}}) = \mathbb{Z}[\zeta_{{p_1}^{\ell_1} \cdots {p_{k-1}}^{\ell_{k-1}}}]$$

Also $\mathbb{A} \cap \mathbb{Q}(\zeta_{p_k^{\ell_k}}) = \mathbb{Z}[\zeta_{p_k^{\ell_k}}]$
Note the compositum of $\mathbb{Q}(\zeta_{{p_1}^{\ell_1} \cdots {p_{k-1}}^{\ell_{k-1}}})$ and $\mathbb{Q}(\zeta_{p_k^{\ell_k}})$ is $\mathbb{Q}(\zeta_n)$. To see this note that by the Euclidean algorithm there exist integers g and h such that $\zeta_n = (\zeta_{{p_1}^{\ell_1} \cdots {p_{k-1}}^{\ell_{k-1}}})^g (\zeta_{p_k^{\ell_k}})^h$.
Thus $\mathbb{Q}(\zeta_n)$ is in the compositum.

But $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \varphi({p_1}^{\ell_1} \cdots {p_{k-1}}^{\ell_{k-1}})\varphi(p_k^{\ell_k})$.
Since $[K : \mathbb{Q}] \leq \varphi({p_1}^{\ell_1} \cdots {p_{k-1}}^{\ell_{k-1}})\varphi(p_k^{\ell_k})$.
Thus since $\mathbb{Q}(\zeta_n) \subseteq K$ we see $K = \mathbb{Q}(\zeta_n)$.
By Theorem 28,

$$\gcd(\text{disc}(\mathbb{Q}(\zeta_{{p_1}^{\ell_1} \cdots {p_{k-1}}^{\ell_{k-1}}}), \text{disc}(\mathbb{Q}(\zeta_{p_k^{\ell_k}})) = 1$$

Thus by Theorem 35,

$$\mathbb{A} \cap \mathbb{Q}(\zeta_n) \subseteq (\mathbb{A} \cap \mathbb{Q}(\zeta_{{p_1}^{\ell_1} \cdots {p_{k-1}}^{\ell_{k-1}}}))(\mathbb{A} \cap \mathbb{Q}(\zeta_{p_k^{\ell_k}}))$$

hence

$$\mathbb{A} \cap \mathbb{Q}(\zeta_n) \subseteq \mathbb{Z}[\zeta_{{p_1}^{\ell_1} \cdots {p_{k-1}}^{\ell_{k-1}}}]\mathbb{Z}[\zeta_{p_k^{\ell_k}}] = \mathbb{Z}[\zeta_n]$$

Since $\mathbb{Z}[\zeta_n] \subseteq \mathbb{A} \cap \mathbb{Q}(\zeta_n)$ we see that $\mathbb{Z}[\zeta_n] = \mathbb{A} \cap \mathbb{Q}(\zeta_n)$. □

---

18. Lecture: Wednesday, February 16, 2000

Basic Problem: How do we compute the discriminant of a number field K?
Say $K = \mathbb{Q}(\theta)$ with $\theta \in \mathbb{A}$. A first step would be to compute $\text{disc}(\theta)$. If $\text{disc}(\theta)$ is squarefree then we have found $\text{disc}(K)$.
We will now give an easy way of computing $\text{disc}(\theta)$. To do so, we introduce the notion of the resultant of two polynomials.

Definition. Let $f(x), g(x) \in \mathbb{C}[x]$ with $f(x) = a_n x^n + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + \cdots + b_1 x + b_0$.
We define the *resultant* of f and g, denoted by $R(f,g)$ by

$$R = R(f,g) = \det \begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & \cdots & \cdots & 0 \\ 0 & a_n & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & & \vdots \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & b_m & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & & \vdots \\ 0 & \cdots & b_m & b_{m-1} & \cdots & \cdots & \cdots & b_0 \end{pmatrix}$$

Note: that $R(f,g)$ is homogeneous of degree m in the a_i's and homogeneous of degree n in the b_j's.
We claim that $R(f,g) = 0 \iff f$ and g have a common factor in $\mathbb{Q}[x]$.
Note: f and g have a common root in $\mathbb{C}$ if and only if there exist h and k in $\mathbb{C}[x]$ with $h(x)f(x) = k(x)g(x)$ with $deg(h) \leq m-1$ and $\deg(k) \leq n-1$

- ($\Rightarrow$) We have $x-\alpha \mid f(x)$ and $x-\alpha \mid g(x)$ in $\mathbb{C}[x]$ for some $\alpha \in \mathbb{C}$. Thus $f(x) = (x-\alpha)k(x)$ and $g(x) = (x-\alpha)h(x)$ with $h, k \in \mathbb{C}[x]$,$\deg(h) \leq m-1$, $\deg(k) \leq n-1$. Then $h(x)f(x) = (x-\alpha)h(x)k(x) = k(x)g(x)$.
- ($\Leftarrow$) If $h(x)f(x) = k(x)g(x)$ with $\deg(k) \leq n-1$ and $\deg(h) \leq m-1$, then on comparing degrees, we se that there is a root of g which is also a root of f.

Let

$$\begin{aligned} h(x) &= c_{m-1}x^{m-1} + \cdots + c_0 \quad \text{with} \quad h \in \mathbb{C}[x] \\ k(x) &= d_{n-1}x^{n-1} + \cdots + d_0 \quad \text{with} \quad k \in \mathbb{C}[x] \end{aligned}$$

Comparing coefficients of x^{n+m-1},x^{n+m-2},...,x^0 on both sides of (*) we find that

$$\begin{aligned} a_n c_{m-1} &= b_m d_{n-1} \\ a_n c_{m-2} + a_{n-1} c_{m-1} &= b_m d_{n-2} + b_{m-1} d_{n-1} \\ &\vdots \\ a_0 c_0 &= b_0 d_0 \end{aligned}$$

We want to find a non-trivial solution to the above system of equations in the variables $c_0, \ldots, c_{m-1}, -d_0, \ldots, -d_{n-1}$.
Since we have $m+n$ equations and $m+n$ unknowns, we can find such a solutions if and only if $\det(A) = 0$ where

$$A = \begin{pmatrix} a_n & & & & 0 & b_m & & & & 0 \\ a_{n-1} & a_n & & & & b_{m-1} & b_m & & & \\ a_{n-2} & a_{n-1} & a_n & & & b_{m-2} & b_{m-1} & b_m & & \\ \vdots & & & \ddots & & & & & \ddots & \\ 0 & & & & a_0 & 0 & & & & b_0 \end{pmatrix}$$

But $\det(A) = det(A^T) = R(f,g)$.

19. Lecture: Friday, February 18, 2000

The coefficients $a_1, \ldots, a_{n-1}$ can be expressed as a_n times an elementary symmetric function of the roots $x_1, \ldots, x_n$ of f.
Similarly the b_j's for $0 \leq j \leq m-1$ are b_m times an elementary symmetric function of the roots $y_1, \ldots, y_n$ of g.
The resultant of f and g is homogenous of degree m in the a_i's and homogenous of degree n in the b_j's. Therefore $R(f,g)$ is ${a_n}^m {b_m}^n$ times a symmetric function of the x_i's times a symmetric function of the y_j's.
We now view x_i's and y_j's as indeterminants and so $R(f,g) \in \mathbb{C}[x_1, \ldots, x_n, y_1, \ldots, y_m]$.
Note that if $x_i = y_j$ then $R(f,g) = 0$ and so $x_i - y_j$ divides R in $\mathbb{C}[x_1, \ldots, x_n, y_1, \ldots, y_m]$. But $x_i - y_j$ is a prime in the UFD $\mathbb{C}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and so S divides R in $\mathbb{C}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ where

$$S = {a_n}^m {b_m}^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j)$$

Observe that since $g(x) = b_m \prod_{j=1}^{m} (x - y_j)$, we see that

$$S = {a_n}^m \prod_{i=1}^{n} g(x_i) \tag{1}$$

Also note that $f(x) = a_n \prod_{i=1}^{n} (x - x_i) = (-1)^n a_n \prod_{i=1}^{n} (x_i - x)$ hence

$$S = (-1)^{mn} {b_m}^n \prod_{j=1}^{m} f(y_i) \tag{2}$$

¿From (1), S is homogenous of degree n in the b_j's and from (2) S is homogenous of degree m in the a_i's.
Thus R and S have the same degree while S divides R. Hence $R = cS$ for some constant c. By the definition of the resultant, we see that

$$R = {a_n}^m {b_m}^n + \cdots$$

while from (1),

$$S = {a_n}^m {b_m}^n + \cdots$$

and so $R = S$.
Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and suppose $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ in $\mathbb{C}[x]$. Then by (1),

$$R(f, f') = \prod_{i=1}^{n} f'(\alpha_i)$$

But

$$f'(x) = \sum_{i=1}^{n} (x - \alpha_1) \cdots \widehat{(x - \alpha_i)} \cdots (x - \alpha_n)$$

where $\widehat{(x - \alpha_i)}$ means that $(x - \alpha_i)$ is removed from the product.
Thus $f'(\alpha_i) = \prod_{\substack{j=1 \\ j \neq i}} (\alpha_i - \alpha_j)$.

Hence

$$R(f,f') = \prod_{i=1}\prod_{\substack{j=1\\ j\neq i}}(\alpha_i - \alpha_j)$$
$$= (-1)^{\frac{n(n-1)}{2}} \prod_{1\leq i\leq j\leq n}(\alpha_i - \alpha_j)^2$$

Suppose that $f \in Z[x]$ is irreducible over $\mathbb{Q}$ and that θ is a root of f. Let $\theta = \theta_1, \ldots, \theta_n$ be the conjugates of θ. Then

$$\operatorname{disc}(\theta) = \prod_{1\leq i\leq j\leq n}(\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} R(f,f')$$

20. Lecture: Monday, February 21, 2000

Example:
Let θ be a root of $f(x) = x^3 + x^2 - 2x + 8$. Note that f is irreducible over $\mathbb{Q}$ by the rational roots theorem. What is disc(θ)?
Observe that

$$f'(x) = 3x^2 + 2x - 2$$

Hence

$$R(f, f') = \det \begin{pmatrix} 1 & 1 & -2 & 8 & 0 \\ 0 & 1 & 1 & -2 & 8 \\ 3 & 2 & -2 & 0 & 0 \\ 0 & 3 & 2 & -2 & 0 \\ 0 & 0 & 3 & 2 & -2 \end{pmatrix}$$

$$= \cdots = \det \begin{pmatrix} -6 & -112 \\ 14 & -74 \end{pmatrix} = 2012 = 4 \cdot 503$$

Thus $\text{disc}(\theta) = (-1)^{\frac{3(3-1)}{2}} 4 \cdot 503 = -4 \cdot 503$.
Put $K = \mathbb{Q}(\theta)$. What is disc(K)? It is either $-4 \cdot 503$ or -503.
If $\{1, \theta, \theta^2\}$ is an integral basis for K, then $\text{disc}(K) = -4 \cdot 503$. We'll show that it isn't by showing that $\frac{\theta^2 - \theta}{2} \in \mathbb{A} \cap K$. We then conclude that $\text{disc}(K) = -503$.
Let $\theta = \theta_1, \theta_2, \theta_3$ be the conjugates of θ. Thus $f(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3)$.
Further, $\frac{\theta^2+\theta}{2} = \frac{{\theta_1}^2+\theta_1}{2}, \frac{{\theta_2}^2+\theta_2}{2}, \frac{{\theta_3}^2+\theta_3}{2}$ are the conjugates of $\frac{\theta^2+\theta}{2}$. Thus

$$g(x) = \left(x - \left(\frac{{\theta_1}^2 + \theta_1}{2}\right)\right)\left(x - \left(\frac{{\theta_2}^2 + \theta_2}{2}\right)\right)\left(x - \left(\frac{{\theta_3}^2 + \theta_3}{2}\right)\right)$$

is the minimal polynomial of $\frac{\theta^2+\theta}{2}$ and it suffices to show that $g \in \mathbb{Z}[x]$.
Note that

$$\left.\begin{array}{lcl} \theta_1 + \theta_2 + \theta_3 & = & -1 \\ \theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 & = & -2 \\ \theta_1\theta_2\theta_3 & = & -8 \end{array}\right\} \text{ since } f(x) = x^3 + x^2 - 2x + 8$$

Thus

$$\frac{{\theta_1}^2 + \theta_1}{2} + \frac{{\theta_2}^2 + \theta_2}{2} + \frac{{\theta_3}^2 + \theta_3}{2} = \frac{{\theta_1}^2 + {\theta_2}^2 + {\theta_3}^2 + \theta_1 + \theta_2 + \theta_3}{2}$$

$$= \frac{(\theta_1 + \theta_2 + \theta_3)^2 - 2(\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3) + (\theta_1 + \theta_2 + \theta_3)}{2}$$

$$= \frac{(-1)^2 - 2(-2) + (-1)}{2} = \frac{4}{2} = 2 \in \mathbb{Z}$$

Next observe that

$$\frac{({\theta_1}^2 + \theta_1)({\theta_2}^2 + \theta_2)}{4} + \frac{({\theta_1}^2 + \theta_1)({\theta_3}^2 + \theta_3)}{4} + \frac{({\theta_2}^2 + \theta_2)({\theta_3}^2 + \theta_3)}{4}$$

$$= \frac{1}{4}({\theta_1}^2{\theta_2}^2 + \theta_1{\theta_2}^2 + {\theta_1}^2\theta_2 + \theta_1\theta_2 + {\theta_1}^2{\theta_3}^2 + \theta_1{\theta_3}^2 + {\theta_1}^2\theta_3 + \theta_1\theta_3 + {\theta_2}^2{\theta_3}^2 + \theta_2{\theta_3}^2 + {\theta_2}^2\theta_3 + \theta_2\theta_3)$$

$$= \frac{1}{4}((\theta_1\theta_2 + \theta_2\theta_3 + \theta_1\theta_3)^2 - 2({\theta_1}^2\theta_2\theta_3 + \theta_1{\theta_2}^2\theta_3 + \theta_1\theta_2{\theta_3}^3) + (\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_2) - 3\theta_1\theta_2\theta_3)$$

$$= \frac{1}{4}(4 - 16 - 2 + 2 + 24)$$

$$= 3 \in \mathbb{Z}$$

Finally,

$$\left(\frac{{\theta_1}^2 + \theta_1}{2}\right)\left(\frac{{\theta_2}^2 + \theta_2}{2}\right)\left(\frac{{\theta_3}^2 + \theta_3}{2}\right) = \frac{\theta_1\theta_2\theta_3}{8}(\theta_1 + 1)(\theta_2 + 1)(\theta_3 + 1)$$

$$= -(\theta_1 + 1)(\theta_2 + 1)(\theta_3 + 1) \in \mathbb{A}$$

Thus $(\frac{{\theta_1}^2+\theta_1}{2})(\frac{{\theta_2}^2+\theta_2}{2})(\frac{{\theta_3}^2+\theta_3}{2})$ is an integer. (In fact, it is equal to 101.)
Therefore $\mathrm{disc}(K) = -503$.

Definition. Let L be a finite extension of $\mathbb{Q}$. Suppose $[L : \mathbb{Q}] = n$. Suppose that $\lambda \in \mathbb{A} \cap L$ and that $\{1, \lambda, \lambda^2, \ldots, \lambda^{n-1}\}$ is an integral basis for L. We say that it is a *power basis*.

Dedekind showed that not all fields L have a power basis. In fact he showed that if $L = K = \mathbb{Q}(\theta)$, as in the example, that K does not have a power basis.

We can check that $\mathrm{disc}(1, \theta, \frac{\theta^2+\theta}{2}) = -503$ and hence that $\{1, \theta, \frac{\theta^2+\theta}{2}\}$ is an integral basis for K.

Suppose $\lambda \in \mathbb{A} \cap K$. We'll show $\mathrm{disc}(\lambda) \neq -503$. Note that

$$\lambda = a + b\theta + c\left(\frac{\theta^2 + \theta}{2}\right) \text{ with } a, b, c \in \mathbb{Z}$$

Thus

$$\lambda^2 = a^2 + b^2\theta^2 + \frac{c^2}{4}(\theta^3 + 2\theta^3 + \theta^2) + 2ab\theta + ac(\theta^2 + \theta) + bc(\theta^3 + \theta^2)$$

We use $\theta^2 = -\theta^2 + 2\theta - 8$ and $\theta^4 = -\theta^3 + 2\theta^2 - 8\theta$.
Hence $\theta^4 + 2\theta^3 + \theta^2 = 2\theta^2 - 6\theta - 8$ and $\theta^3 + \theta^2 = 2\theta - 8$.
Thus $\lambda^2 = A_1 + A_2\theta + A_3\left(\frac{\theta^2+\theta}{2}\right)$ where

$$\begin{aligned} A_1 &= a^2 - 2c^2 - 8bc \\ A_2 &= -2c^2 + 2ab + 2bc - b^2 \\ A_3 &= 2b^2 + 2ac + c^2 \end{aligned}$$

Therefore

$$\begin{pmatrix} 1 \\ \lambda \\ \lambda^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ A_1 & A_2 & A_3 \end{pmatrix} \begin{pmatrix} 1 \\ \theta \\ \frac{\theta^2+\theta}{2} \end{pmatrix}$$

$$\mathrm{disc}(\lambda) = \det \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ A_1 & A_2 & A_3 \end{pmatrix}^2 \cdot (-503)$$

But we have

$$\det \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ A_1 & A_2 & A_3 \end{pmatrix}^2 = (bA_3 - cA_2)^2 = (2b^3 - bc^2 + b^2c + 2c^3)^2 \equiv (c(b^2 - bc))^2 \equiv 0 \pmod 2$$

Thus $\text{disc}(\lambda) \neq -503$ and so no power integral basis for K exists.

---

21. Lecture: Wednesday, February 23, 2000

Let K be a finite extension of $\mathbb{Q}$. The irreducible elements of $\mathbb{A} \cap K$ are those $\alpha \in \mathbb{A} \cap K$, which are not zero or a unit, for which $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathbb{A} \cap K$ implies that β or γ is a unit. The irreducible elements in $\mathbb{Z} = \mathbb{A} \cap \mathbb{Q}$ are the primes.
In $\mathbb{Z}$ we have the Fundamental Theorem of Arithmetic. In general there is no analogue of this result for $\mathbb{A} \cap K$ with irreducibles taking the role of the primes. (Recall Assignment 2 Question 1, where we showed that in $\mathbb{Z}(\sqrt{-5}) = \mathbb{A} \cap \mathbb{Q}(\sqrt{-5})$ there is not unique factorization into irreducibles.)
However, we can recover unique factorization by passing to ideals.

Definition. A *Dedekind domain* is an integral domain R for which:

1) Every ideal in R is finitely generated.
2) Every prime ideal is a maximal ideal.
3) R is integrally closed in its field of fractions.

We'll show that if K is a finite extension of $\mathbb{Q}$ then $\mathbb{A} \cap K$ is a Dedekind domain. Also, we have unique factorization, up to reordering of ideals, into prime ideals in a Dedekind domain.

Remark.

i) The field of fractions of a ring R is $\{\frac{a}{b} \mid a, b, \in R, b \neq 0\}$.
ii) An element θ in a ring extension S of R is said to be integral over R if it is the root of a monic polynomial with coefficients in R.
iii) A ring R in an extension ring S of R is said to be integrally closed if whenever $\theta \in S$ and θ is integral over R, then $\theta \in R$.

Proposition 37. *Let K be a finite extension of $\mathbb{Q}$. Let I be a nonzero ideal in $\mathbb{A} \cap K$. Then there is a nonzero integer a in I.*

Proof:
Since I is nonzero there is an element $\alpha \in I$ with $\alpha \neq 0$.
Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α.
Then $N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = \alpha_1 \cdots \alpha_n \in \mathbb{Z} \setminus \{0\}$, say $N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = a$.
Note that $\alpha_2 \cdots \alpha_n \in \mathbb{A}$ and $\alpha_2 \cdots \alpha_n = \frac{a}{\alpha} \in \mathbb{Q}(\alpha) \subseteq K$.
Thus $\alpha_2 \cdots \alpha_n \in \mathbb{A} \cap K$. Therefore $\alpha(\alpha_2 \cdots \alpha_n) \in I$. □

Definition. Let K be a finite extension of $\mathbb{Q}$ and let I be an ideal in $\mathbb{A} \cap K$. A set of elements $\{\alpha_1, \ldots, \alpha_n\}$ from I is said to be an *integral basis for I* if for every element of I has a unique representation as an integer linear combination of $\alpha_1, \ldots, \alpha_n$.

Theorem 38. *Let K be a finite extension of $\mathbb{Q}$ and let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis for K. Let I be a nonzero ideal in $\mathbb{A} \cap K$. Then there is an integral basis $\{\alpha_1, \ldots, \alpha_n\}$ for I for*

which

$$\begin{aligned}\alpha_1 &= a_{1,1}\omega_1\\ \alpha_2 &= a_{2,1}\omega_1 + a_{2,2}\omega_2\\ &\vdots\\ \alpha_n &= a_{n,1}\omega_1 + \cdots + a_{n,n}\omega_n\end{aligned} \qquad \textit{with } a_{i,j} \in \mathbb{Z} \textit{ and } a_{i,i} \in \mathbb{Z}^+ \textit{ for } i = 1, \ldots, n$$

Proof:
It follows from Prop. 37 that there is a positive integer a in I. Thus $a\omega_i \in I$ for $i = 1, \ldots, n$. Now take α_1 to be $a_{1,1}\omega_1$ where $a_{1,1}$ is the smallest positive integer for which $a_{1,1}\omega_1$ is in I. We then choose $\alpha_2, \ldots, \alpha_n$ so that $\alpha_i = a_{i,1}\omega_1 + \cdots + a_{i,i}\omega_i$ where $a_{i,i} \in \mathbb{Z}^+$ and $a_{i,1}, \ldots, a_{i,i-1}$ are in $\mathbb{Z}$ with $a_{i,i}$ minimal, for $i = 1, \ldots, n$.

We claim $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis for I. Since $\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & & 0 \\ \vdots & & \ddots & \\ a_{n1} & \cdots & & a_{nn} \end{pmatrix}$ has determinant $a_{11} \cdots a_{nn} \neq 0$ we see that $\alpha_1, \ldots, \alpha_n$ is a basis for K. Thus it suffices to prove that every element β of I has a representation as an integral linear combination of $\alpha_1, \ldots, \alpha_n$. Since $\omega_1, \ldots, \omega_n$ is an integral basis for K, there exist integers $b_1, \ldots, b_n$ such that $\beta = b_1\omega_1 + \cdots + b_n\omega_n$.

Note: that b_n is divisible by a_{nn} by the minimality of a_{nn}. For otherwise, we would have $b_n = qa_{nn} + r$ with $0 < r < a_{nn}$ and then $\beta - q\alpha_n \in I$ and when expressed as a linear combination of $\omega_1, \ldots, \omega_n$, the coefficient of ω_n is positive and smaller than a_{nn}. This contradicts the minimality of a_{nn}.

Thus $b_n = qa_{nn}$ with $q_n \in \mathbb{Z}$. We then consider $\beta - q_n\alpha_n = c_1\omega_1 + \cdots c_{n-1}\omega_{n-1}$. By the minimality of $a_{n-1,n-1}$ we see that $a_{n-1,n-1}$ divides c_{n-1} as before.
Continuing as before we find that $\beta = q_1\alpha_1 + \cdots + q_n\alpha_n$ with $q_1, \ldots, q_n$ integers. □

22. Lecture: Monday, February 28, 2000

Theorem 39. *Let K be a finite extension of $\mathbb{Q}$. Then $\mathbb{A} \cap K$ is a Dedekind domain.*

Proof:
It follows from Theorem 38 that every ideal in $\mathbb{A} \cap K$ is finitely generated.
To show that every prime ideal $\mathcal{P}$ is maximal, we first note that $(\mathbb{A} \cap K)/\mathcal{P}$ is an integral domain. Secondly we observe that if $(\mathbb{A} \cap K)/\mathcal{P}$ is finite, then $(\mathbb{A} \cap K)/\mathcal{P}$ is a field since every finite integral domain is a field. If $(\mathbb{A} \cap K)/\mathcal{P}$ is a field, then $\mathcal{P}$ is maximal.
Thus, it is enough to show that $(\mathbb{A} \cap K)/\mathcal{P}$ is finite.
By Proposition 37, there is a positive integer a in $\mathcal{P}$. Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis for $\mathbb{A} \cap K$.
Note that every element in $\mathbb{A} \cap K$ is an integer linear combination of $\omega_1, \ldots, \omega_n$ and that $a \in \mathcal{P}$. Thus

$$|(\mathbb{A} \cap K)/\mathcal{P}| \leq a^n$$

Finally, let $\gamma = \frac{\alpha}{\beta}$ with $\alpha, \beta \in \mathbb{A} \cap L, \beta \neq 0$.
Suppose that γ is the root of monic polynomial with coefficients in $\mathbb{A} \cap K$, say

$$x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 \text{ with } \alpha_0, \ldots, \alpha_{n-1} \in \mathbb{A} \cap K$$

Since $\gamma = \frac{\alpha}{\beta}$ we see that $\gamma \in K$. It suffices to show that $\gamma \in \mathbb{A}$.
By Theorem 13 we need only show that γ is an element of a subring of $\mathbb{C}$ which has a finitely generated additive subgroup.
Consider $S = \mathbb{Z}[\alpha_0, \ldots, \alpha_{n-1}, \gamma]$. We claim that the additive subgroup of S is finitely generated. Let $[K : \mathbb{Q}] = n$, and let $\theta \in S$.
We'll show that θ is an integral linear combination of terms of the form

$$\alpha_0{}^{j_0} \cdots \alpha_{m-1}{}^{j_{m-1}} \gamma^{j_m} \text{ where } 0 \leq j_i < n \text{ for } i = 0, \ldots, m-1$$

Observe that it suffices to prove that when

$$\theta = \alpha_0{}^{b_0} \cdots \alpha_{n-1}{}^{b_{n-1}} \gamma^{b_m} \text{ with } b_i \geq 0 \text{ for } i = 0, \ldots, m$$

¿From the relation $\gamma^m = \alpha_{m-1}\gamma^{m-1} \cdots \alpha_0$ we can show that γ^{b_m} is an integral linear combination of terms of the form

$$\theta = \alpha_0{}^{\ell_0} \cdots \alpha_{n-1}{}^{\ell_{n-1}} \gamma^{\ell_m}$$

with $0 < \ell_m < m$ and with $\alpha_i \geq 0$ for $i = 0, \ldots, m-1$.
Let

$$f_i(x) = x^{t_i} + a^{(i)}_{t_{i-1}} x^{t_{i-1}} + \cdots + a^{(i)}_0$$

where $a^{(i)}_j \in \mathbb{Z}$ is the minimal polynomial of α_i for $i = 0, \ldots, m$.
We now reduce the powers of the α_i's using the relations given by the minimal polynomial to give the result claimed. □

23. Lecture: Friday, March 3, 2000

Theorem 40. *Let R be a commutative ring. The following are equivalent:*

(1) *Every ideal in R is finitely generated.*
(2) *Every increasing sequence of ideals in R is eventually constant.*
(3) *Every nonempty set of ideals in R has a maximal element.*

Proof:

- $[(1) \implies (2)]$
  Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be a sequence of ideals in R.
  Let
  $$I = \cup_{n=1}^{\infty} I_n$$
  then I is an ideal of R and $I_n \subseteq I$ for $n = 1, 2, \ldots$. Since every ideal in R is finitely generated there exist $a_1, \ldots, a_r \in R$ such that
  $$I = (a_1, \ldots, a_r)$$
  Thus $a_i \in I_{n_i}$ for some integer n_i for $i = 1, \ldots, r$.
  Let $N = \max(n_1, \ldots, n_r)$. Then
  $$I \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq I$$
  and so $I = I_N = I_{N+1} = \cdots$ as required.
- $[(2) \implies (3)]$
  Let S be a nonempty set of ideals in R. Let I_1 be an ideal of S.
  Either I_1 is maximal or there exists I_2 in S with $I_1 \subsetneq I_2$. Similarly, either I_n is maximal or there exists $I_{n+1} \in S$ with $I_n \subsetneq I_{n+1}$.
  By (2), this sequence terminates after finitely many steps.
  The last term in the sequence is a maximal element of S.
- $[(3) \implies (1)]$
  Let I be an ideal of R.
  Let S be the set of ideals contained in I which are finitely generated. S is nonempty and so by (3) contains a maximal element M.
  Notice that $M = I$, since otherwise $M \subsetneq I$, and then there exists an element $\beta \in M \setminus I$. Suppose $M = (\alpha_1, \ldots, \alpha_n)$. Then $M_1 = (\alpha_1, \ldots, \alpha_n, \beta)$ is in S and $M \subsetneq M_1$ which contradicts the fact that M is a maximal element of S. Then $M = I$ and so I is finitely generated.

□

Lemma 41. *In a Dedekind domain R, every nonzero ideal of R contains a product of prime ideals from R.*

Proof:
Let S be the set of nonzero ideals in R which do not contain a product of prime ideals from R. If S is nonempty then, by (1) and (3) of Theorem 40, S contains a maximal element M. M is not prime and thus there exist $r, s \in R \setminus M$ with $rs \in M$. Consider
$$M_1 = M + (r), \qquad M_2 = M + (s)$$
Since M is maximal in S, $M \subsetneq M_1$ and $M \subsetneq M_2$, so we see that M_1 and M_2 are not in S and so both M_1 and M_2 contain a product of prime ideals from R.

But $M_1M_2 \subseteq M$, and thus M contains a product of prime ideals, which is a contradiction. Thus S is empty. □

Lemma 42. *Let I be a proper ideal in a Dedekind domain R. Let K denote the field of fractions of R. Then there exists an element $\gamma \in K$ with $\gamma \notin R$ such that $\gamma I \subseteq R$.*

Proof:
Note that we may assume I is nonzero, since the result holds for any $\gamma \in K \setminus R$ in the case of $I = (0)$. So let a be a nonzero element of I.
Since I is proper, a is not a unit, and so $\frac{1}{a} \notin R$, while $\frac{1}{a} \in K$.
By Lemma 41, (a) contains a product of prime ideals, $\mathcal{P}_1, \ldots, \mathcal{P}_r$, from R. Choose such a product with r minimal. We have

$$\mathcal{P}_1 \cdots \mathcal{P}_r \subseteq (a)$$

Let S be the set of proper ideals containing I.
Then S is nonempty. since $I \in S$ and so, since R is a Dedekind domain, S contains a maximal element M.
Note that M is a maximal ideal of R and so M is a prime ideal of R.
Thus $M \supseteq \mathcal{P}_1 \cdots \mathcal{P}_r$. Observe that $M \supset \mathcal{P}_i$ for some i with $1 \leq i \leq r$.
(To see this, note that if this were not true, then there is an element $a_i \in \mathcal{P}_i$ with $a_i \notin M$ for $i = 1, \ldots, r$.
But then $a_1 \cdots a_r \in M$ and this contradicts the fact that M is a prime ideal.)
Without loss of generality, we may suppose that $M \supseteq \mathcal{P}_1$. (In fact $M = \mathcal{P}_1$ since R is a Dedekind domain.)
Recall that $(\alpha) \supseteq \mathcal{P}_1 \cdots \mathcal{P}_r$ and that r is minimal.
If $r = 1$ we take $\gamma = \frac{1}{\alpha}$ then since $\mathcal{P}_1 \subseteq (\alpha) \subseteq I \nsubseteq R$ and prime ideals in Dedekind domains are maximal ideals then

$$\mathcal{P}_1 = (\alpha) = I$$
$$\gamma I = \frac{1}{\alpha}(\alpha) = R$$

as required.
If $r > 1$ we choose an element b in $\mathcal{P}_2 \cdots \mathcal{P}_r$ and take $\gamma = \frac{b}{\alpha}$. Note that $\mathcal{P}_2 \cdots \mathcal{P}_r$ is not contained in (α) since r is minimal.
Thus $\gamma \in K \setminus R$. Then

$$\gamma I = \frac{b}{\alpha} I \subseteq \frac{b}{\alpha}\mathcal{P}_1 \subseteq \frac{(b)\mathcal{P}_1}{\alpha} \subseteq \frac{\mathcal{P}_2 \cdots \mathcal{P}_r \mathcal{P}_1}{\alpha} \subseteq \frac{(\alpha)}{\alpha} = R$$

as required. □

24. Lecture: Monday, March 6, 2000

Theorem 43. *Let R be a Dedekind domain and let I be an ideal of R. Then there exists an ideal J such that IJ is principal.*

Proof:
If $I = (0)$ result is immediate. So, suppose $I \neq (0)$.
Let $\alpha \in I \setminus \{0\}$. Put

$$J = \{\beta \in R \mid \beta I \subseteq (\alpha)\}$$

Note that J is an ideal and that $JI \subseteq (\alpha)$.
It remains to show $(\alpha) \subseteq IJ$ hence that $(\alpha) = IJ$.
Put $B = \frac{1}{\alpha} IJ$. Then B is an ideal of R.
If B is a proper ideal of R then by Lemma 42, there exists $\gamma \in K \setminus R$ such that $\gamma B \not\subseteq R$.
Since $\alpha \in I$ we see that $J \subseteq B$. Thus $\gamma J \subseteq \gamma B \subseteq R$.
Note that since $\gamma B \subseteq R$ we see that $\gamma JI = (\alpha)$. Therefore, by the definition of J, $\gamma J \subseteq J$.
Now J has a finitely generated additive subgroup and, as in the proof of Theorem 13 for Dedekind domains, $\gamma \in R$.
The contradiction proves the result. □

25. Lecture: Wednesday, March 8, 2000

Corollary 44. *If A, B, C are ideals with $C \neq 0$ in a Dedekind domain and $AC = BC$, then $A = B$.*

Proof:
There exists an ideal J such that $JC = (\alpha)$ for some nonzero element α. Thus

$$JAC = JBC \implies (\alpha)A = (\alpha)B \implies \alpha A = \alpha B$$

Hence, since $\alpha \neq 0$, then $A = B$. □

Corollary 45. *Let A and B be ideals in Dedekind domain R. Then $A \supseteq B \iff A \mid B$.*

Proof:

($\Leftarrow$) If $A \mid B$ then there exists C such that $AC = B$ implies $A \supseteq B$.
($\Rightarrow$) Suppose $A \supseteq B$. The result holds with $A = (0)$ so assume $A \neq (0)$.
Then there exists an ideal J such that $JA = (\alpha)$ with $\alpha \neq 0$.
Then $JA = (\alpha) \supseteq JB$, hence $R \supseteq \frac{1}{\alpha}$.
Let $C = \frac{1}{\alpha} JB$. Note C is an ideal and $AC = B$.

□

Theorem 46. *Every proper nonzero ideal in a Dedekind domain has a unique factorization, up to reordering, into a product of prime ideals.*

Proof:
Let S be the set of nonzero proper ideals in R which cannot be written as a product of prime ideals.
If S is not empty, there is a maximal element $M \in S$.
Notice that M is contained in a maximal ideal $\mathcal{P}$ of R. Since $M \in S$, then $M \not\subseteq P$. By Corollary 45, there exists an ideal C such that $M = \mathcal{P}C$.
Since $M \in S$, C is not a product of prime ideals. So $C \in S$ and $C \supseteq M$, which is a contradiction.
Thus S is empty. Now we show the factorization is unique up to reordering. Suppose that

$$\mathcal{P}_1 \cdots \mathcal{P}_r = Q_1 \cdots Q_s$$

with $\mathcal{P}_1, \ldots, \mathcal{P}_r$ and $Q_1, \ldots, Q_s$ prime ideals.
Then $\mathcal{P}_1 \mid Q_1 \cdots Q_s$ hence $\mathcal{P}_1 \supseteq Q_1 \ldots Q_s$.
Since $\mathcal{P}_1$ is a prime ideal $\mathcal{P}_1 \supseteq Q_i$ for some $1 \leq i \leq s$.
Without loss of generality, we may suppose $i = 1$, so that $\mathcal{P}_1 \supseteq Q_1$. In a Dedekind domain, prime ideals are maximal ideals, so $\mathcal{P}_1 = Q_1$.
By Corollary 44,

$$\mathcal{P}_2 \cdots \mathcal{P}_r = Q_2 \cdots Q_s$$

The result follows by induction. □

Remark. Let $[K : \mathbb{Q}]$ be finite. Since the ring of algebraic integers of K is a Dedekind domain, we have unique factorization into prime ideals in $\mathbb{A} \cap K$.

---

26. Lecture: Friday, March 10, 2000

Theorem 47. *Let $[K : \mathbb{Q}] < \infty$. Factorization of elements of $\mathbb{A} \cap K$ into primes is unique up to reordering if and only if every ideal in $\mathbb{A} \cap K$ is principal.*

Proof:

($\Rightarrow$) : It suffices to prove every prime ideal is principal. Let $\mathcal{P}$ be a prime ideal of $\mathbb{A} \cap K$. By By Proposition 37, $\mathcal{P}$ contains a nonzero rational integer a. Therefore $\mathcal{P} \supseteq (a)$. Accordingly $\mathcal{P} \mid (a)$. Let $a = \pi_1 \cdots \pi_t$ be a representation of a as a product of primes of $\mathbb{A} \cap K$. (Note: $a \neq \pm 1$ since $\mathcal{P}$ is a prime ideal.) Thus

$$(a) = (\pi_1) \cdots (\pi_t)$$

and since $\mathcal{P} \mid (a)$ we see that $\mathcal{P} \mid (\pi_i)$ for some i with $1 \leq i \leq t$. Without loss of generality, we may suppose $\mathcal{P} \mid (\pi_1)$.
If we can show (π_1) is a prime ideal then $\mathcal{P} = (\pi_1)$ and the result follows.
Suppose $\beta\gamma \in (\pi_1)$ with $\beta, \gamma \in \mathbb{A} \cap K$. Then $\pi_1 \mid \beta\gamma$ and on examining the prime factorization of β and γ we see that $\pi_1 \mid \beta$ or $\pi_1 \mid \gamma$. Thus (π_1) is a prime ideal.

($\Leftarrow$) : Assume $\pi_1 \cdots \pi_r = \lambda_1 \cdots \lambda_s$ with $\pi_1, \ldots, \pi_r, \lambda_1, \ldots, \lambda_s$ primes in $\mathbb{A} \cap K$. Then

$$(\pi_1) \cdots (\pi_r) = (\lambda_1) \cdots (\lambda_s)$$

It suffices to show that if π is a prime in $\mathbb{A} \cap K$ then (π) is a prime ideal since the result then follows from the above equality and the fact the in $\mathbb{A} \cap K$ we have unique

factorization into prime ideals.
Suppose $(\pi) = BC$ for some ideals B and C in $\mathbb{A} \cap K$. Since every ideal is principal in $\mathbb{A} \cap K$ we have $B = (\beta)$, $C = (\gamma)$ for β, γ in $\mathbb{A} \cap K$.
Thus $(\pi) = (\beta)(\gamma) = (\beta\gamma)$. In other words, $\frac{\pi}{\beta\alpha}$ is a unit. Since π is a prime we see that either β or γ is a unit and thus B or C is (1), hence (π) is a prime ideal.

□

Let $K = \mathbb{Q}(\sqrt{-D})$ where D is a squarefree positive integer. Gauss conjectured that $\mathbb{A} \cap K$ had unique factorization into primes only if $D = 1, 2, 3, 7, 11, 19, 43, 67, 163$.
In 1934 Heilbrann proved that there is at most one more D other than those in Gauss' list.
In 1969 Baker and Stark independently proved that the above is a complete list.
Let K be a finite extension of $\mathbb{Q}$ and let $\mathcal{P}$ be a prime ideal of $\mathbb{A} \cap K$. Let a be a positive integer in $\mathbb{A} \cap K$. Note $a > 1$.
Let $a = p_1 \cdots p_r$ with $p_1, \ldots, p_r$ primes in $\mathbb{Z}$.
Then $(a) = (p_1) \cdots (p_r)$, hence $\mathcal{P} \supseteq (a)$ or $\mathcal{P} \mid (a)$ hence $\mathcal{P} \mid (p_i)$ for some prime p_i.
In fact there is only one such prime p. Suppose $\mathcal{P} \mid (q)$ also with q a prime in $\mathbb{Z}$ different from p. There there exist integers a and b such that

$$ap + bq = 1$$

hence

$$(a)(p) + (b)(q) = (1)$$

and then $\mathcal{P} \mid (1)$ which is a contradiction.
Thus to determine all prime ideals of $\mathbb{A} \cap K$ it suffices to determine the prime ideal decomposition of (p) in $\mathbb{A} \cap K$ as p ranges over the rational primes.

27. Lecture: Monday, March 13, 2000

Definition. Let K be a finite extension of $\mathbb{Q}$, and let p be a prime in $\mathbb{Z}$. We say that p be a prime in $\mathbb{Z}$. We say that p *ramifies* in K if there is a prime ideal $\mathcal{P}$ in $\mathbb{A} \cap K$ such that $\mathcal{P}^2 \mid (p)$ in $\mathbb{A} \cap K$.

Dedekind proved that p ramifies in K if and only if p divides the discriminant of K.

Theorem 48. *Let K be a finite extension of $\mathbb{Q}$ and let D be the discriminant of K. If p is a prime in $\mathbb{Z}$ and $p \nmid D$ then p is unramified.*

Proof:
Suppose $\mathcal{P}^2 \mid (p)$ for some prime ideal $\mathcal{P}$ in $\mathbb{A} \cap K$ and some p in $\mathbb{Z}$.
Then $(p) = \mathcal{P}^2 Q$ for some ideal Q in $\mathbb{A} \cap K$. Let $\alpha \in \mathcal{P}Q$ with $\alpha \notin \mathcal{P}^2 Q$ so that $\frac{\alpha}{p} \in A \cap K$.
Note that $\alpha^2 \in \mathcal{P}^2 Q^2 \subseteq (p)$ so $\frac{\alpha^2}{p} \in \mathbb{A} \cap K$. Therefore, for any $\beta \in \mathbb{A} \cap K$, $\frac{(\alpha\beta)^p}{p} \in \mathbb{A} \cap K$.
Further,

$$T_Q^K((\alpha\beta)^p) = T_Q^K(p\frac{(\alpha\beta)^p}{p}) = pT_Q^K(\frac{(\alpha\beta)^p}{p})$$

and so $p \mid T_Q^K((\alpha\beta)^p)$. Further,

$$\begin{aligned}(T_Q^K(\alpha\beta))^p &= (\sum_\sigma \sigma(\alpha\beta))^p, \ \sigma \text{ an embedding from } K \text{ to } Q \\ &= \sum_\sigma \sigma(\alpha\beta)^p + p\gamma \text{ for } \gamma \in \mathbb{A} \cap K \\ &= \sum_\sigma \sigma((\alpha\beta)^p) + p\gamma \\ &= T_Q^K((\alpha\beta)^p) + p\gamma\end{aligned}$$

Therefore, $p \mid (T_Q^K(\alpha\beta))^p$, hence $p \mid T_Q^K(\alpha\beta)$.
Let $\omega_1, \ldots, \omega_n$ be an integral basis for K.
We have $\alpha = a_1\omega_1 + \cdots + a_n\omega_n$ for some $a_1, \ldots, a_n \in \mathbb{Z}$. Since $\alpha \notin (p)$, we see that $p \nmid a_i$ for some i with $1 \le i \le n$. Without loss of generality, we may suppose $p \nmid a_1$.
By our earlier remarks, we see that $p \nmid T_Q^K(\alpha\omega_i)$ for $i = 1, \ldots, n$.
Thus $p \mid T_Q^K(a_1\omega_1 + \cdots + a_n\omega_n)\omega_1$ so $p \mid \sum_{j=1}^n a_k T_Q^K(\omega_j\omega_i)$.
Denote T_Q^K by T. Then

$$a_1 D = \det \begin{pmatrix} a_1T(\omega_1\omega_1) & \cdots & a_1T(\omega_1\omega_n) \\ T(\omega_2\omega_1) & \cdots & T(\omega_2\omega_n) \\ \vdots & & \vdots \\ T(\omega_n\omega_1) & \cdots & T(\omega_n\omega_n) \end{pmatrix}$$

$$= \det \begin{pmatrix} a_1T(\omega_1\omega_1) + \cdots + a_nT(\omega_n\omega_1) & \cdots & a_1T(\omega_1\omega_n) + \cdots + a_nT(\omega_n\omega_n) \\ T(\omega_2\omega_1) & \cdots & T(\omega_2\omega_n) \\ \vdots & & \vdots \\ T(\omega_n\omega_1) & \cdots & T(\omega_n\omega_n) \end{pmatrix}$$

Thus by (*), we have $p \mid a_1 D$. Since $p \nmid a_1$, we see that $p \mid D$ and the result follows. $\square$

28. Lecture: Wednesday, March 15, 2000

Let $[K:\mathbb{Q}] < \infty$. Let $\alpha \in \mathbb{A} \cap K$. We have defined the norm of α, $N_{\mathbb{Q}}^K(\alpha)$. We now extend this notion to ideals.

Definition. We define the *norm of an ideal* I in $\mathbb{A} \cap K$, denoted $N(I)$ or $N_{\mathbb{Q}}^K(I)$ or $\|I\|$ to be $|(\mathbb{A} \cap K)/I|$. In other words, $N(I)$ is the number of cosets mod I in $\mathbb{A} \cap K$ or the number of residue classes modulo I in $\mathbb{A} \cap K$.

Theorem 49. *Let K be a finite extension of $\mathbb{Q}$ and let I be an ideal in $\mathbb{A} \cap K$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis for I. Then*

$$N(I) = \left| \frac{\operatorname{disc}(\alpha_1, \ldots, \alpha_n)}{D} \right|^{\frac{1}{2}} \quad \textit{where } D = \operatorname{disc}(K)$$

Proof:
Every integral basis for I has the same discriminant.
Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis for $\mathbb{A} \cap K$ and $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis for I of the form given by Theorem 38.

$$\text{Then } \operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \left(\det \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & & 0 \\ \vdots & & \ddots & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix} \right)^2 \operatorname{disc}(\omega_1, \ldots, \omega_n)$$

$$\implies \frac{\operatorname{disc}(\alpha_1, \ldots, \alpha_n)}{D} = (a_{11} \cdots a_{nn})^2$$

Recall $a_{ii} \in \mathbb{Z}^+$ for $i = 1, \ldots, n$. Hence

$$\left| \frac{\operatorname{disc}(\alpha_1, \ldots, \alpha_n)}{D} \right|^{\frac{1}{2}} = a_{11} \cdots a_{nn}$$

Thus it suffices to prove that $N(I) = a_{11} \cdots a_{nn}$.
First we show that if

$$r_1\omega_1 + \cdots + r_n\omega_n \equiv s_1\omega_1 + \cdots + s_n\omega_n \pmod{I}$$

with $0 \le r_i \le a_{ii}$ and $0 \le s_i \le a_{ii}$ for $i = 1, \ldots, n$.
Then $r_i = s_i$ for $i = 1, \ldots, n$. This shows $N(I) \ge a_{11} \cdots a_{nn}$.
Note $(r_1 - s_1)\omega_1 + \cdots + (r_n - s_n)\omega_n \in I$.
Recall from the proof of Theorem 38 that a_{nn} was the smallest positive integer occurring as the coefficient of ω_n in a linear combination of $\omega_1, \ldots, \omega_n$ which is in I.
Therefore $a_{nn} \mid r_n - s_n$ and since $0 \le r_n \le a_{nn}$ and $0 \le s_n \le a_{nn}$ we see $r_n = s_n$.
Similarly $a_{n-1,n-1} \mid r_{n-1} - s_{n-1}$ and so $r_{n-1} = s_{n-1}, \ldots, r_1 = s_1$.
Thus $N(I) \ge a_{11} \cdots a_{nn}$.

Let $\gamma \in \mathbb{A} \cap K$ so $\gamma = b_1\omega_1 + \cdots + b_n\omega_n$ with $b_1, \ldots, b_n \in \mathbb{Z}$. Then there exist integers $q_1, \ldots, a_n$ and $r_1, \ldots, r_n$ with $0 \leq r_i \leq a_{ii}$ for $i = 1, \ldots, n$ such that

$$\gamma = q_1\alpha_{11} + \cdots + q_n\alpha_{nn}r_1\omega_1 + \cdots + r_n\omega_n$$

But then $\gamma \equiv r_1\omega_1 + \cdots + r_n\omega_n \pmod{I}$.
Thus $N(I) \leq a_{11} \cdots a_{nn}$.
Therefore $N(I) = a_{11} \cdots a_{nn}$.

□

Theorem 50. *Let K be a finite extension of $\mathbb{Q}$ and let I be a principal ideal of $\mathbb{A} \cap K$. Suppose $I = (\alpha)$. Then*

$$N(I) = \left|N_{\mathbb{Q}}^K(\alpha)\right|$$

Proof:
Let $\omega_1, \ldots, \omega_n$ be an integral basis for $\mathbb{A} \cap K$.
Then $\alpha\omega_1, \ldots, \alpha\omega_n$ be an integral basis for I.
Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$. We have

$$\begin{pmatrix} \sigma_1(\alpha\omega_1) & \cdots & \sigma_1(\alpha\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha\omega_1) & \cdots & \sigma_n(\alpha\omega_n) \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) & & 0 \\ & \ddots & \\ 0 & & \sigma_n(\alpha) \end{pmatrix} \begin{pmatrix} \sigma_1(\omega_1) & \cdots & \sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \cdots & \sigma_n(\omega_n) \end{pmatrix}$$

Thus by Theorem 49,

$$N(I) = \left|\left(\det \begin{pmatrix} \sigma_1(\alpha) & & 0 \\ & \ddots & \\ 0 & & \sigma_n(\alpha) \end{pmatrix}\right)^2\right|^{\frac{1}{2}} = \left|N_{\mathbb{Q}}^K(\alpha)\right|$$

□

---

29. Lecture: Friday, March 17, 2000

Theorem 51 (Fermat's Theorem)**.** *Let $[K : \mathbb{Q}] < \infty$ and let $\mathcal{P}$ be a prime ideal of $\mathbb{A} \cap K$. Let $\alpha \in \mathbb{A} \cap K$ such that $\mathcal{P} \not| (\alpha)$. Then $\alpha^{N(\mathcal{P})-1} \equiv 1 \pmod{\mathcal{P}}$.*

Proof:
Let $\beta_1, \ldots, \beta_{N(\mathcal{P})}$ be a complete set of residues modulo $\mathcal{P}$ and suppose that $\beta_{N(\mathcal{P})} \equiv 0 \pmod{\mathcal{P}}$.
Then $\alpha\beta_1, \ldots, \alpha\beta_{N(\mathcal{P})}$ is also a complete set of residues modulo $\mathcal{P}$ since if $\alpha\beta_i \equiv \alpha\beta_j \pmod{\mathcal{P}}$, then $\mathcal{P} \mid (\alpha)(\beta_i - \beta_j)$ and so $\mathcal{P} \mid (\beta_i - \beta_j)$.
Thus $\beta_i \equiv \beta_j \pmod{\mathcal{P}}$ and so $i = j$.
Thus we see that $(\alpha\beta_1)(\alpha\beta_2)\cdots(\alpha\beta_{N(\mathcal{P})-1}) \equiv \beta_1\beta_2\cdots\beta_{N(\mathcal{P})-1} \pmod{\mathcal{P}}$ so

$$\alpha^{N(\mathcal{P})-1}(\beta_1 \cdots \beta_{N(\mathcal{P})-1}) \equiv \beta_1 \cdots \beta_{N(\mathcal{P})-1} \pmod{\mathcal{P}}$$

and therefore

$$\alpha^{N(\mathcal{P})-1} \equiv 1 \pmod{\mathcal{P}}$$

□

Proposition 52. *Let $[K:\mathbb{Q}] < \infty$ and let I be an ideal of $\mathbb{A} \cap K$. Then $N(I) \in I$.*

Proof:
Let $\alpha_1, \ldots, \alpha_{N(I)}$ be a complete set of residues modulo I. Then

$$1+\alpha_1, 1+\alpha_2, \ldots, 1+\alpha_{N(I)}$$

is also a complete set of residues modulo I.
Therefore,

$$(1+\alpha_1) + \cdots + (1+\alpha_{N(I)}) \equiv \alpha_1 + \cdots + \alpha_{N(I)} \pmod{I}$$

hence

$$N(I) \equiv 0 \pmod{I}$$

as required. □

Remark. It follows immediately from Proposition 52 that if K is a finite extension of $\mathbb{Q}$, then for each positive integer a there are only finitely many ideals in $\mathbb{A} \cap K$ with norm equal to a.
Note that if we can show the norm is multiplicative on ideals of $\mathbb{A} \cap K$. then we can conclude:

(1) If $N(I)$ is a prime in $\mathbb{Z}$ then I is a prime ideal; for if $I = AB$, then $N(I) = N(A) \cdot N(B)$, hence either $N(A) = 1$ or $N(B) = 1$.
(2) If $\mathcal{P}$ is a prime ideal in $\mathbb{A} \cap K$ with $[K:\mathbb{Q}] = n$ and $\mathcal{P} \mid (p)$ with p a prime in $\mathbb{Z}$ then $N(\mathcal{P}) \mid p^n$ hence $N(\mathcal{P}) = p^f$ for some f with $1 \le f \le n$.

Definition. Let $[K:\mathbb{Q}] < \infty$ and let B and C be ideals in $\mathbb{A} \cap K$. We say that D is the *greatest common divisor (of ideals)* B and C if

$$D \mid B \text{ and } D \mid C$$

and whenever $E \mid B$ and $E \mid C$, then $E \mid D$.

Note that if a greatest common divisor exists, then it is uniquely determined since if D and E are greatest common divisors of A and B then $D \mid E$ and $E \mid D$ hence $E \subseteq D$ and $D \subseteq E$. So $E = D$.
Suppose that $B = (\alpha_1, \ldots, \alpha_r)$ and $C = (\beta_1, \ldots, \beta_s)$. Then $D = (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$ is the greatest common divisor of B and C.
To see this, note that $B \subseteq D$ since $\alpha_1, \ldots, \alpha_r$ are in D, and so $D \mid B$. Similarly $D \mid C$.
If E is a common divisor of B and C, then $E \mid B$ so E contains $\beta_1, \ldots, \beta_s$. Thus

$$E \supseteq (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s) = D$$

so $E \mid D$.
Therefore D is in fact the greatest common divisor of A and B. We denote this by $\gcd(A, B)$ or (A, B).
Alternatively, if $\mathcal{P}_1, \ldots, \mathcal{P}_r$ are the distinct prime ideals which divide AB and

$$A = {\mathcal{P}_1}^{e_1} \cdots {\mathcal{P}_r}^{e_r} \text{ with } 0 \le e_i \text{ for } i = 1, \ldots, r$$

and

$$B = {\mathcal{P}_1}^{f_1} \cdots {\mathcal{P}_r}^{f_r} \text{ with } 0 \le f_j \text{ for } j = 1, \ldots, r$$

then

$$\gcd(A,B) = \mathcal{P}_1^{\min(e_1,f_1)} \cdots \mathcal{P}_r^{\min(e_r,f_r)}$$

Definition. If $\gcd(A,B) = (1)$, then we say that A and B are *relatively prime (as ideals)*
Note if $(\alpha) = BL$ then we denote L by $\frac{(\alpha)}{B}$.

Lemma 53. *Let $[K:\mathbb{Q}] < \infty$ and let B and C be nonzero ideals in $\mathbb{A} \cap K$. Then there is an element $\alpha \in B$ such that $\gcd(\frac{(\alpha)}{B}, C) = (1)$.*

Proof:
Note that if $C = (1)$ then any α in B will do.
If $C \neq (1)$, then we can express C as a nonempty product of prime ideals of $\mathbb{A} \cap K$.
Let $\mathcal{P}_1, \ldots, \mathcal{P}_r$ be the distinct prime powers of C. The argument proceeds by induction on r.
First consider the case $r = 1$. In this case we choose α in B but not in $B\mathcal{P}_1$.
Such a choice is possible since otherwise $B = B\mathcal{P}_1$, hence $\mathcal{P}_1 = (1)$ which is a contradiction.
We have $(\alpha) = BE$ for some ideal E in $\mathbb{A} \cap K$ since $B \supseteq (\alpha)$ hence $B \mid (\alpha)$. Thus $\frac{(\alpha)}{B} = E$ and it suffices to show that $\mathcal{P}_1 \nmid E$.
Note that if $\gcd(E,C) = \mathcal{P}_1$m then $E = \mathcal{P}_1 F$ and thus $(\alpha) = BE = B\mathcal{P}_1 F$.
In particular, $B\mathcal{P}_1 \mid (\alpha)$ hence $B\mathcal{P}_1 \supseteq (\alpha)$ and so $\alpha \in B\mathcal{P}_1$ which is a contradiction. The result follows for $r = 1$.
Let $\mathcal{P}_1, \ldots, \mathcal{P}_r$ be the distinct prime ideals dividing C.
We prove the result by induction on r.
We now make the inductive assumption that the result follows holds for $q \leq k \leq r$.
Let

$$B_m = B\mathcal{P}_1 \cdots \widehat{\mathcal{P}_m} \cdots \mathcal{P}_r = B\frac{\mathcal{P}_1 \cdots \mathcal{P}_r}{\mathcal{P}_m}$$

for $m = 1, \ldots, r$.
We can find an element α_m in B_m for $m = 1, \ldots, r$ such that $\gcd(\frac{(\alpha_m)}{B_m}, B_m) = 1$ by our inductive hypothesis. Put

$$\alpha = \alpha_1 + \cdots + \alpha_r$$

Since $B \supset B_m$ for $m = 1, \ldots, r$ we have that $\alpha \in B$. Note that $\alpha \notin B\mathcal{P}_m$ for $m = 1, \ldots, r$. To see this, observe that $\alpha \in B\mathcal{P}_m$ for some m with $1 \leq m \leq r$, then since $\alpha_i \in B\mathcal{P}_m$ for $i \neq m$, we find that $\alpha_m \in B\mathcal{P}_m$.
Thus $(\alpha_m) \subseteq B\mathcal{P}_m$ hence $B\mathcal{P}_m \mid (\alpha_m)$. Therefore $\mathcal{P}_m \mid \frac{(\alpha_m)}{B}$.
Since $\mathcal{P}_1, \ldots, \mathcal{P}_r$ are distinct prime ideals, we see that $\mathcal{P}_m \mid \frac{(\alpha_m)}{B_m}$ and this contradicts the that that $\gcd(\frac{(\alpha)}{B_m}, \mathcal{P}_m) = 1$.
Suppose now that $\gcd(\frac{(\alpha)}{B}, C) \neq 1$. Then

$$\mathcal{P}_m \mid \gcd\left(\frac{(\alpha)}{B_m}, \mathcal{P}_m\right) \text{ for some } n \text{ for } 1 \leq m \leq r$$

Thus $\mathcal{P}_m \mid \frac{(\alpha)}{B}$ or equivalently $B\mathcal{P}_m \mid (\alpha)$. Thus $B\mathcal{P} \supset (\alpha)$ and so $\alpha \in B\mathcal{P}_m$ which is a contradiction. Thus $\gcd(\frac{(\alpha)}{C}) = (1)$. $\square$

30. Lecture: Monday, March 20, 2000

Theorem 54. *Let $[K : \mathbb{Q}] < \infty$ and let B and C be ideals in $\mathbb{A} \cap K$. Then $N(BC) = N(B)N(C)$.*

Proof:
By Lemma 53 there is an element $\gamma \in B$ such that $\gcd(\frac{\gamma}{B}, C) = 1$.
Let $\alpha_1, \ldots, \alpha_{N(B)}$ be a complete set of residues modulo B, and let $\beta_1, \ldots, \beta_{N(C)}$ be a complete set of residues modulo C.
Note that the numbers $\alpha_i + \gamma B_j$ are distinct modulo B for $1 \leq i \leq N(B)$ and $1 \leq j \leq N(C)$. To see this, suppose $\alpha_i + \gamma\beta_j = \alpha_k + \gamma\beta_\ell \pmod{BC}$. Then

$$\alpha_i - \alpha_k = \gamma(\beta_\ell - \beta_j) \pmod{BC}$$

Thus $\alpha_i - \alpha_j \equiv 0 \pmod{B}$ and so $i = k$. Therefore,

$$\gamma(\beta_\ell - \beta_j) \equiv 0 \pmod{BC}$$

Since $\gcd(\frac{(\gamma)}{B}, C) = 1$ we see that $\gcd((\gamma), BC) =$. Thus $\beta_\ell - \beta_j \equiv 0 \pmod{C}$, hence $\ell = j$. Therefore, $N(BC) \geq N(B)N(C)$.
Pick $\alpha \in \mathbb{A} \cap K$. Then it remains to show that

$$\alpha = \alpha_i + \gamma\beta_j \pmod{BC} \text{ for } i, j \text{ with } 1 \leq i \leq N(B),\ 1 \leq j \leq N(C)$$

Now $\alpha \equiv \alpha_i \pmod{B}$ for some i with $1 \leq i \leq N(B)$. Since $\alpha - \alpha_i$ is in B and since $\gcd((\gamma), BC) = B$ we can write $\alpha - \alpha_i$ in the form $\gamma\beta + \lambda$ with $\beta \in \mathbb{A} \cap K$ and $\lambda \in BC$. Then we put $\beta \equiv \beta_j \pmod{C}$ with $1 \leq i \leq N(C)$ and we find that

$$\alpha - \alpha_j = \gamma\beta_j + \gamma(\beta - \beta_j) + \lambda$$

Since $\beta - \beta_j \in C$ and $\gcd((\gamma), BC) = B$ we see that

$$\gamma(\beta - \beta_j) + \lambda \in BC$$

and hence that

$$\alpha \equiv \alpha_i + \gamma\beta_j \pmod{BC}$$

Therefore $N(B) \cdot N(C) \geq N(BC)$ and so $N(B) \cdot N(C) = N(BC)$. □

31. Lecture: Wednesday, March 22, 2000

Definition. Let $[K : \mathbb{Q}] < \infty$. Let A and B be ideals in $\mathbb{A} \cap K$. We define a relation $\sim$ on the ideals of $\mathbb{A} \cap K$ in the following way: we write $A \sim B$ if there exist nonzero elements α and β of $\mathbb{A} \cap K$ such that $(\alpha)A = (\beta)B$.

Note that $\sim$ is an equivalence relation since:

(1) $A \sim A$ since $A = (1)A = A(1)$.
(2) If $A \sim B$, then there exist $\alpha, \beta \in \mathbb{A} \cap K$ with $\alpha\beta \neq 0$ such that $(\alpha)A = (\beta)B$. But then $(\beta)B = (\alpha)A$ so $B \sim A$.

(3) If $A \sim B$ and $B \sim C$, then there exist α, β such that $(\alpha)A = (\beta)B$ and there exist γ, δ such that $(\gamma)B = (\delta)C$.
Therefore,
$$(\gamma)(\alpha)A = (\gamma)(\beta)B = (\beta)(\delta)C$$
so $(\gamma\alpha)A = (\beta\delta)C$ and thus $A \sim C$.

Definition. The equivalence classes under $\sim$ are known as *ideal classes*. The number of equivalence classes, denoted by h or h_K, is called the *class number* of K.

If $h = 1$, then all of the ideals of $\mathbb{A} \cap K$ are principal. To see this, note that if B is an ideal of $\mathbb{A} \cap K$, then $B \sim (1)$. Thus there exist $\alpha, \beta \in \mathbb{A} \cap K$ with $\alpha, \beta \neq 0$ such that $(\alpha)(1) = (\beta)B$. In other words, $(\alpha) = (\beta)B$.
Note that $\alpha \in (\alpha)$ and the elements of the right hand side are of the form $\beta\theta$ with $\theta \in \mathbb{A} \cap K$. Thus $\frac{\alpha}{\beta} \in \mathbb{A} \cap K$. Note that $(\alpha) = (\beta)(\frac{\alpha}{\beta})$.
Thus $(\beta)B = (\beta)(\frac{\alpha}{\beta})$ hence $B = \frac{\alpha}{\beta}$.
We next define the binary operation of multiplication on the set of ideal classes.

Definition. Let $[K : \mathbb{Q}]$, and let A, B be ideals in $\mathbb{A} \cap K$. Denote the ideal classes of which A and B are representatives by $[A]$ and $[B]$ respectively. Then we define $\cdot$ by
$$[A] \cdot [B] = [AB]$$
We must now check that this multiplication is well-defined. So suppose that $A \sim C$ and $B \sim D$; then we must show that $AB \sim CD$.
Since $A \sim C$, there exist $\alpha, \gamma \in \mathbb{A} \cap K, \alpha\beta \neq 0$ with $(\alpha)A = (\gamma)C$; and since $B \sim D$, there exist $\beta, \delta \in \mathbb{A} \cap K, \beta, \delta \neq 0$ with $(\beta)B = (\delta)D$.
But then
$$(\alpha)A \cdot (\beta)B = (\gamma)C \cdot (\delta)D$$
and hence $(\alpha\gamma)AB = (\beta\delta)CD$ and so $AB \sim CD$.

Let $\mathcal{C} = \{[A] \mid A \neq 0, A \text{ an ideal of } \mathbb{A} \cap K\}$.
With the above definition of multiplication, $\mathcal{C}$ is an abelian group. Let us check the properties:

(1) Associativity: $[A] \cdot ([B] \cdot [C]) = [A] \cdot [BC] = [A(BC)] = [ABC] = [(AB)C] = [AB] \cdot [C] = ([A] \cdot [B]) \cdot [C]$
(2) Identity element: $[(1)] \cdot [B] = [B] = [B] \cdot [(1)]$.
(3) Inverses: Consider $[B]$. Let b be an integer in B. Then $B \supseteq (b)$, so there exists C such that $BC = (b)$.
Then the ideal class $[B] \cdot [C] = [(b)] = [(1)]$.

Then $\mathcal{C}$ is a group under $\cdot$.
It is abelian since $[A][B] = [B][A]$.

Definition. $\mathcal{C}$ is called the *ideal class group* of K.

32. Lecture: Friday, March 24, 2000

Theorem 55. *Let $[K:\mathbb{Q}] < \infty$. Let A be an ideal in $\mathbb{A} \cap K$. Then there exists a positive number c_0 and an element $\alpha \in A$ with $\alpha \neq 0$ such that*

$$\left|N_{\mathbb{Q}}^{K}(\alpha)\right| \leq c_0 N(A)$$

(Note: c_0 depends on K but not on A.)

Proof:
Let $\omega_1, \ldots, \omega_n$ be an integral basis for K. Put $t = [(NA)^{(1/n)}]$; here $n = [K:\mathbb{Q}]$.
Consider the number β of the form

$$\beta = c_1\omega_1 + \cdots + c_n\omega_n \text{ where } 0 \leq c_i \leq t \text{ for } i = 1, \ldots, n$$

There are $(t+1)^n > N(A)$ such numbers and so two of them, β_1 and β_2 say, are congruent modulo A. So let

$$\alpha = \beta_1 - \beta_2 = t_1\omega_1 + \cdots + t_n\omega_n \text{ with } |t_i| \leq t$$

Note that $\alpha \in A$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$. Then

$$\begin{aligned}
\left|N_{\mathbb{Q}}^{K}(\alpha)\right| &= \left|\prod_{j=1}^{n} \sigma_j(\alpha)\right| \\
&= \left|\prod_{j=1}^{n} (t_1\sigma_j(\omega_1) + \cdots + t_n\sigma_j(\omega_n))\right| \\
&\leq \prod_{j=1}^{n} (|t_1|\,|\sigma_j(\omega_1)| + \cdots + |t_n|\,|\sigma_j(\omega_n)|) \\
&\leq t^n \prod_{j=1}^{n} (|\sigma_j(\omega_1)| + \cdots + |\sigma_j(\omega_n)|) \\
&\leq (N(A))c_0 \text{ where } c_0 = \prod_{j=1}^{n} (|\sigma_j(\omega_1)| + \cdots + |\sigma_j(\omega_n)|)
\end{aligned}$$

Note that $\alpha \neq 0$ since $\beta_1 \neq \beta_2$.

□

We'll show later that we can take $c_0 = \sqrt{|D|}$.

Theorem 56. *Let $[K:\mathbb{Q}] < \infty$. The class number h of K is finite.*

Proof:
We'll show that every ideal class of $\mathbb{A} \cap K$ contains an ideal of $\mathbb{A} \cap K$ of norm at most c_0; c_0 from Theorem 55.
Since there are only finitely many ideals of a given norm, the result forms.
Let I be an ideal in $\mathbb{A} \cap K$. Then there is an ideal A in $\mathbb{A} \cap K$ such that

$$IA \sim (1) \tag{1}$$

By Theorem 55 there is an element $\alpha \in A$ with $\alpha \neq 0$, $\left|N_{\mathbb{Q}}^{K}(\alpha)\right| \leq c_0 N(A)$.
Recall that $\left|N_{\mathbb{Q}}^{K}(\alpha)\right| = N(\alpha)$.
Since $\alpha \in A$ there exists an ideal B with $AB = (\alpha)$. Thus

$$BA \sim (1) \tag{2}$$

¿From (1) and (2) we see that $B \sim I$. But since the norm function is multiplicative on ideals, then

$$N(A) \cdot N(B) = N(AB) = N(\alpha) \leq c_0 N(A)$$

Hence $N(B) \leq c_0$ as required. □

Remark. Let $[K : \mathbb{Q}] < \infty$. Let A and B be ideals in $\mathbb{A} \cap K$. Then $[A^h] = [(1)]$ by Lagrange's Theorem.
Further, if q if a positive integer with $(q, h) = 1$ and if

$$[A^q] = [B^q] \text{ then } [A] = [B]$$

To see this note that there are integers r and s such that $rq - sh = 1$.
Then note that

$$[A^{qr}] = [B^{qr}] \text{ hence } [AA^{sh}] = [BB^{sh}]$$

and so by our previous result, we have $[A] = [B]$.

33. Lecture: Monday, March 27, 2000

Example:
Let us determine the ideal class group $\mathcal{C}$ of $\mathbb{Q}(\sqrt{-23})$. (We'll assume $c_0 \leq \sqrt{|D|}$ in Theorem 55).
Since $-23 \equiv 1 \pmod 4$ we see that $c_0 \leq \sqrt{23}$ and so we need only consider ideals of norm at most 4 as possible representatives of the different ideal classes.
We have

$$(2) = (2, \tfrac{1+\sqrt{-23}}{2})(2, \tfrac{1-\sqrt{-23}}{2}) = \mathcal{P}\mathcal{P}'$$

say and note that $\mathcal{P}$ and $\mathcal{P}'$ are prime ideals since they have norm 2.
Also,

$$(3) = (3, \tfrac{1-\sqrt{-23}}{2})(3, \tfrac{1+\sqrt{-23}}{2}) = \mathcal{Q}\mathcal{Q}'$$

where $\mathcal{Q}, \mathcal{Q}'$ are prime ideals.
Thus the ideals of $\mathbb{A} \cap K$ of norm at most 4, are

$$(1), \mathcal{P}, \mathcal{P}', \mathcal{Q}, \mathcal{Q}', \mathcal{P}\mathcal{P}', \mathcal{P}^2, \mathcal{P}'^2$$

Note that $\mathcal{P}\mathcal{P}' = (2) \sim (1)$.
Consider

$$N_{\mathbb{Q}}^{Q}(\sqrt{-23})(\tfrac{a+b\sqrt{-23}}{2}) = 2$$

then $a^2 + 23b^2 = 8$, hence $b = 0$. But then $a^2 = 8$, which is a contradiction. Thus there is no principal ideal of norm 2.
Therefore,

$$\mathcal{P} \not\sim (1), \qquad \mathcal{P}' \not\sim (1)$$

Further,

$$\mathcal{P}\mathcal{Q} = (6, 2(\tfrac{1-\sqrt{-23}}{2}), 3(\tfrac{1-\sqrt{-23}}{2}), (\tfrac{1-\sqrt{-23}}{2})^2)$$

Since $(\frac{1-\sqrt{-23}}{2})(\frac{1+\sqrt{-23}}{2}) = 6$ we see that $\mathcal{P}\mathcal{Q} = (\frac{1-\sqrt{-23}}{2})$ and so $\mathcal{P}\mathcal{Q} \sim (1)$.
Similarly, $\mathcal{P}'\mathcal{Q}' = (\frac{1+\sqrt{-23}}{2})$ and so $\mathcal{P}'\mathcal{Q}' \sim (1)$.
Therefore $\mathcal{P}\mathcal{P}'\mathcal{Q}' \sim \mathcal{P}$ hence $\mathcal{Q}' \sim \mathcal{P}$ (since $\mathcal{P}\mathcal{P}' \sim (2)$) and also we have $\mathcal{P}'\mathcal{P}\mathcal{Q} \sim \mathcal{P}'$ hence $\mathcal{Q} \sim \mathcal{P}'$.
This leaves us with

$$(1), \mathcal{P}, \mathcal{P}', \mathcal{P}^2, \mathcal{P}'^2$$

Notice that $N(\frac{3+\sqrt{-23}}{2}) = 8 = N(\frac{3-\sqrt{-23}}{2})$.
Observe that $(\frac{3+\sqrt{-23}}{2})/(\frac{3-\sqrt{-23}}{2})$ is not a unit in $\mathbb{Q}(\sqrt{-23})$, hence there are at least 2 distinct principal ideals of norm 8. The ideals of norm 8 are:

$$\mathcal{P}^3, \mathcal{P}^2\mathcal{P}', \mathcal{P}\mathcal{P}'^2, \mathcal{P}'^3$$

Note that $\mathcal{P}^2\mathcal{P}' \not\sim (1)$ since $\mathcal{P} \not\sim (1)$, and $\mathcal{P}'^2\mathcal{P} \not\sim (1)$ since $\mathcal{P}' \not\sim (1)$.
Thus $\mathcal{P}^3$ and $\mathcal{P}'^3$ are principal so $\mathcal{P}^3 \sim (1)$ and $\mathcal{P}'^3 \sim (1)$.
Thus $\mathcal{P}'\mathcal{P}^3 \sim \mathcal{P}'$ hence $\mathcal{P}^2 \sim \mathcal{P}'$.

Also $\mathcal{P}\mathcal{P}'^3 \sim \mathcal{P}$ hence $\mathcal{P}'^2 \sim \mathcal{P}$.
Thus we are left with

$$(1), \mathcal{P}, \text{ and } \mathcal{P}^2$$

as possible representatives of distinct ideal classes.
Note $\mathcal{P} \not\sim (1)$. Also $\mathcal{P}^2 \not\sim (1)$ since otherwise

$$\mathcal{P}^2 \sim (1) \implies \mathcal{P}^3 \sim \mathcal{P} \implies \mathcal{P} \sim (1), \text{ since } \mathcal{P}^3 \sim (1)$$

This a contradiction.
Further, $\mathcal{P}^2 \sim \mathcal{P}$ since otherwise $\mathcal{P} \sim (1)$, which is a contradiction.
Thus $h = 3$ and $\mathcal{C} \cong \mathbb{Z}/3\mathbb{Z}$.

Hilbert conjectured and Furtivangler proved the following:
Let $[K : \mathbb{Q}] < \infty$. There exists an extension E of K with the following properties:

(1) $[E : K] = h_K$
(2) E is Galois over K.
(3) The ideal class group of K is isomorphic to the Galois group of E over K.
(4) Every ideal of $\mathbb{A} \cap K$ becomes a principal ideal of $\mathbb{A} \cap E$.
(5) Every prime ideal $\mathcal{P}$ of $\mathbb{A} \cap K$ decomposes into the product of $\frac{h_K}{f}$ prime ideals in $\mathbb{A} \cap E$ where f is the order of $[\mathcal{P}]$ in the ideal class group of $\mathbb{A} \cap E$.

There is a unique field E satisfying $1, \dots, 5$ and it is known as the *Hilbert class field* of K.

Lattices

Let $\alpha_1, \dots, \alpha_n$ be vectors in $\mathbb{R}^n$ which are linearly independent over $\mathbb{R}$.
The set of all points of the form

$$u_1\alpha_1 + \cdots + u_n\alpha_n, \text{ with } u_i \in \mathbb{Z} \text{ for } i = 1, \dots, n$$

denoted Λ, is a lattice in $\mathbb{R}^n$, with basis $\alpha_1, \dots, \alpha_n$.
Notice that the basis $\alpha_1, \dots, \alpha_n$ is not uniquely determined by Λ. Let

$$\alpha_i' = \sum_{j=1}^{n} v_{i,j}\alpha_j \tag{1}$$

where the $v_{i,j}$'s are integers with $\det((v_{i,j})) = \pm 1$.
Then

$$\alpha_i = \sum_{j=1}^{n} w_{i,j}\alpha_j' \tag{2}$$

where the $w_{i,j}$'s are integers and $\det((w_{i,j})) = \pm 1$.
Then

$$\begin{aligned}\Lambda &= \{u_1\alpha_1 \cdots + u_n\alpha_n \mid u_i\mathbb{Z}, i = 1, \dots, n\} \\ &= \{u_1\alpha_1' \cdots + u_n\alpha_n' \mid u_i\mathbb{Z}, i = 1, \dots, n\}\end{aligned}$$

Thus $\alpha_1', \dots, \alpha_n'$ is also a basis for Λ. In fact, if $\{\alpha_1, \dots, \alpha_n\}$ and $\{\alpha_1', \dots, \alpha_n'\}$ are bases for Λ, then (1) and (2) hold for some choice of integers $v_{i,j}$ and $w_{i,j}$.
To see that $\det((v_{i,j})) = \pm 1$ and $\det((w_{i,j})) = \pm 1$ we can substitute (2) into (1) and note

that α_i' has a unique representation as an integral linear combination of $\alpha_1', \ldots, \alpha_n'$ as α_i'. Thus

$$\sum_j v_{i,j} w_{j,k} = \begin{cases} 1 & \text{if } i = k \\ 0 & \text{otherwise} \end{cases}$$

Thus

$$\det(v_{i,j}) \det(w_{j,k}) = \det \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = 1$$

Since $v_{i,j}, w_{j,k} \in \mathbb{Z}$ we see that $\det((v_{i,j})) = \pm 1$ and $\det((w_{j,k})) = \pm 1$.
Thus if $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\alpha_1', \ldots, \alpha_n'\}$ are bases for Λ then

$$\det(\alpha_1, \ldots, \alpha_n = \det(\alpha_1', \ldots, \alpha_n')$$

and so we can define $d(\Lambda)$, the determinant of Λ, by

$$d(\Lambda) = |\det(\alpha_1, \ldots, \alpha_n)|$$

Example:

$$\Lambda_0 = \{(u_1, \ldots, u_n) \in \mathbb{R}^n \mid u_i \in \mathbb{Z} \text{ for } i = 1, \ldots, n\}$$
$$d(\Lambda_0) = 1$$

---

34. Lecture: Wednesday, March 29, 2000

Theorem 57 (Blichfeldt's Theorem)**.** *Let $m, n \in \mathbb{Z}^+$, let Λ be a lattice in $\mathbb{R}^n$ and let S be a set in $\mathbb{R}^n$ with Lebesgue measure $\mu(S)$.*
Suppose

$$\mu(S) > md(\Lambda)$$
$$\text{or } \mu(S) \geq md(\Lambda) \text{ and } S \text{ is compact}$$

Then there exist $m+1$ distinct points $x_1, \ldots, x_{m+1}$ in S such that all differences $x_i - x_j$ are in Λ, for $1 \leq i, j \leq m+1$.

Proof:
Let $\alpha_1, \ldots, \alpha_n$ be a basis for Λ and put

$$P = \{\alpha_1\theta_1 + \cdots + \alpha_n\theta_n \mid 0 \leq \theta_i < 1 \text{ for } i = 1, \ldots, n\}$$

Note that every point x in $\mathbb{R}^n$ has a unique representation of the form $\lambda + \gamma$ with $\lambda \in \Lambda$ and $\gamma \in P$. Also note that $\mu(P) = d(\Lambda)$.
For $\lambda \in \Lambda$ we let $R(\lambda)$ denote that set of points $\nu \in P$ such that $\lambda + \nu \in S$. Then

$$\sum_{\lambda \in \Lambda} \mu(R(\lambda)) = \mu(S) \tag{1}$$

Suppose now that $\mu(S) > md(\Lambda)$ hence that $\mu(S) > m\mu(P)$, so

$$\sum_{\lambda \in \Lambda} \mu(R(\lambda)) > m\mu(P)$$

Thus there is a point ν_0 in P which occurs in at least $m+1$ set $r(\lambda)$. In particular, there exist $\lambda_1, \ldots, \lambda_{m+1} \in \Lambda$ such that $\nu_0 + \lambda_i \in S$ for $i = 1, \ldots, m+1$.
Then put $x_i = \lambda_i + \nu_0$ for $i = 1, \ldots, m+1$, we find that

$$x_i - x_j \in \Lambda \setminus \{0\} \text{ for } i \neq j$$

We now consider the case where $\mu(S) = md(\Lambda)$ and S is compact.
Let $\epsilon_1, \ldots$ be a sequence of decreasing positive real numbers tending to 0.
Then consider $S_r = (1+\epsilon_r)S$. Notice that

$$\mu(S_r) = (1+\epsilon_r)^n \mu(S) > \mu(S)$$

so that we can apply the first part of the theorem to get distinct points $x_{j,r}$ in S_r for $j = 1, \ldots, m+1$ whose differences are in Λ.
Since S is compact in $\mathbb{R}^n$ it is closed and bounded. We can extract a subsequence of the indices r such that on the subsequence the $x_{j,r}$'s converge to $x'_j \in S$ for $i = 1, \ldots, m+1$.
Notice that $x_{j,r} - x_{i,r} \in \Lambda$ for each r and that Λ is discrete. Thus for $r > r_0$, $x_{j,r} - x_{i,r}$ is constant.
Therefore, $x'_j - x'_i \in \Lambda$. □

Definition. A subset S of $\mathbb{R}^n$ is *symmetric* about the origin if whenever x is in S then $-x$ is in S.
A subset S of $\mathbb{R}^n$ is *convex* if whenever x and y are in S then for all $\lambda \in \mathbb{R}$ with $0 \leq \lambda \leq 1$, we have $\lambda x + (1-\lambda)y \in S$

Theorem 58 (Minkowski's Theorem)**.** *Let $m, n \in \mathbb{Z}^+$ and let Λ be a lattice in $\mathbb{R}^n$. Let S be a subset of $\mathbb{R}^n$ with Lebesgue measure $\mu(S)$. Suppose that S is convex and symmetric about the origin. If either*

$$\mu(S) > m2^n d(\Lambda)$$
$$\text{or } \mu(S) = m2^n d(\Lambda) \text{ and } S \text{ is compact}$$

then there exist m pairs $\pm\lambda_j$ for $j = 1, \ldots, m$ of lattice points, different from $\vec{0}$, in S.

Proof:
We first apply Theorem 57 to the set $\frac{1}{2}S$.
It has volume $\mu(\frac{1}{2}S) = \frac{1}{2^n}\mu(S)$, hence by Theorem 57 there exist $m+1$ points $\frac{1}{2}x_1, \ldots, \frac{1}{2}x_{m+1}$ in $\frac{1}{2}S$ such that the differences $\frac{1}{2}x_i - \frac{1}{2}x_j$ are in Λ. Note that $\frac{1}{2}x_i - \frac{1}{2}x_j \neq 0$ for $i \neq j$.
We order the x_i's, $x_1 > x_2 > \ldots > x_{m+1}$ so that $x_i > x_j$ whenever the first nonzero coordinate of $x_i - x_j$ (reading from left to right) is positive.
Take $\lambda_j = \frac{1}{2}x_j - \frac{1}{2}x_{m+1}$ for $j = 1, \ldots, m$.
Then $\pm\lambda_1, \ldots, \pm\lambda_m$ are all distinct. Further, $-\frac{1}{2}x_{m+1} \in S$ since S is symmetric about the origin.
Further, since S is convex,

$$\lambda_j = \frac{1}{2}x_j + \frac{1}{2}(-x_{m+1}) \in S \text{ for } j = 1, \ldots, m$$

□

Remark. Minkowski's Theorem is best possible, as the following example shows:
Let $m, n \in \mathbb{Z}^+$. Put $S = \{(x_1, \dots, x_n) \in R^n \mid |x_1| < m, |x_j| \text{ for } j = 2, \dots, n\}$
Then $\mu(S) = m2^n = m2^n d(\Lambda_0)$ where $\Lambda_0 = \{(u_1, \dots, u_n) \mid u_i \in \mathbb{Z} \text{ for } i = 1, \dots, n\}$ the only lattice points of Λ_0 in S different from 0 are $\pm(i, 0, \dots, 0)$ for $i = 1, \dots, m-1$.

---

35. Lecture: Friday, March 31, 2000

Let $[K : \mathbb{Q}] = n$. Suppose $K = \mathbb{Q}(\theta)$ for $\theta \in K$. Let $\theta = \theta_1, \dots, \theta_n$ be the conjugates of θ.
There are n distinct embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$, say $\sigma_1, \dots, \sigma_n$. They are determined from the fact that $\sigma_i(\theta) = \theta_i$ for $i = 1, \dots, n$.
We may suppose that $\sigma_i : K \to \mathbb{R}$ for $i = 1, \dots, n$ and that σ_i is not an embedding in $\mathbb{R}$ for $i = r_1 + 1, \dots, r_1 + r_2$, and we may suppose that $\sigma_{r_1+i} = \overline{\sigma_{r_1+r_2+i}}$ for $i = 1, \dots, r_2$.
For any $x \in K$ we define $\sigma(x)$ by

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_{r_1+r_2}(x))$$

Now we have $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ and σ is an injective ring homomorphism. We can identify $\mathbb{C}$ with $\mathbb{R}^2$ in the usual way and so view σ as a map from K to $\mathbb{R}^n$. With this assumption we have:

Lemma 59. *Let A be a non-zero ideal in $\mathbb{A} \cap K$. Then $\sigma(A)$ is a lattice Λ in $\mathbb{R}^n$, and*

$$d(\Lambda) = 2^{-r_2} |D|^{1/2} N(A)$$

Proof:
Let $\alpha_1, \dots, \alpha_n$ be an integral basis for A. The co-ordinates of $\sigma(\alpha_i)$ with respect to the canonical basis for $\mathbb{R}^n$ are given by

$$(\sigma_1(\alpha_i), \dots, \sigma_{r_1}(\alpha_i), \mathrm{Re}(\sigma_{r_1+1}(\alpha_i)), \mathrm{Im}(\sigma_{r_1+1}(\alpha_i)), \dots, \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_i)))$$

Let D_0 be the determinant of the matrix whose ith row is given above.
Notice that

$$D_0 = \left(\frac{1}{-2i}\right)^{r_2} \det(\sigma_j(\alpha_i))$$

since for any $z \in \mathbb{C}$, $\mathrm{Re}(z) = \frac{z+\overline{z}}{z}$ and $\mathrm{Im}(z) = \frac{z-\overline{z}}{zi}$.
But by Theorem 49, we have

$$\det(\sigma_j(\alpha_i)) = |D|^{1/2} N(A)$$

Thus $D_0 \neq 0$ so $\sigma(A)$ is a lattice Λ in $\mathbb{R}^n$ and

$$d(\Lambda) = |D_0| = \frac{1}{2^{r_2}} |D|^{1/2} N(A)$$

as required. □

Theorem 60. *Let A be a non-zero ideal in $\mathbb{A} \cap K$. Then there exists a non-zero element α in A for which*

$$\left|N_{\mathbb{Q}}^K(\alpha)\right| \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|D|}\, N(A)$$

Proof:
Let $t \in \mathbb{R}^+$ and define S_t by

$$\begin{aligned} S_t &= \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid |x_i| \leq t \text{ for } i = 1, \ldots, r_1 \\ &\quad \text{and } x_{r_1+2j+1}^2 + x_{r_1+2j+2}^2 \leq t^2 \text{ for } j = 0, \ldots, r_2 - 1\} \end{aligned}$$

Note that S_t is convex and symmetric about the origin and

$$\mu(S_t) = 2^{r_1}\pi^{r_2}t^n$$

Now, we choose t so that

$$2^{r_1}\pi^{r_2}t^n = 2^n \frac{1}{2^{r_2}} |D|^{1/2} N(A)$$

so

$$t = \left(\left(\frac{2}{\pi}\right)^{r_2} |D|^{1/2} N(A)\right)^{1/n}$$

Then by Minkowski's Theorem there is a non-zero lattice point of $\sigma(A)$ in S_t. Let α be the corresponding element in A.
Then

$$\begin{aligned} \left|N_{\mathbb{Q}}^K(\alpha)\right| &= \left|\prod_{i=1}^{n} \sigma_i(\alpha)\right| = \left|\prod_{i=1}^{r_1} \sigma_i(\alpha)\right| \cdot \left|\prod_{i=1}^{r_2} \sigma_{r_1+i}(\alpha)\overline{\sigma_{r_1+i}(\alpha)}\right| \\ &= \left|\prod_{i=1}^{r_1} \sigma_i(\alpha)\right| \cdot \prod_{j=1}^{r_2} (\mathrm{Re}(\sigma_{r_1+j}(\alpha))^2 + \mathrm{Im}(\sigma_{r_1+j}(\alpha))^2) \\ &\leq t^n = \left(\frac{2}{\pi}\right)^{r_2} |D|^{1/2} N(A) \end{aligned}$$

□

Remark. If we choose S_t to be $S_t = \{(x_1, \ldots, x_n) \mid \sum_{i=1}^n |x_i| \leq t\}$ and use the arithmetic-geometric mean inequality, we can sharpen Theorem 60 to

$$\left|N_{\mathbb{Q}}^K(\alpha)\right| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D|^{1/2} N(A)$$

Index