PMATH 641 Lecture 1: January 7, 2013

Cam Stewart MC 5051
Algebraic Number Theory
Marks: Final exam 65%
Midterm 25%
Assignments 10%
Grad Students: essay & talk
No text.
Notes on my webpage.
Reference Texts: Number Fields: Marcus
Algebraic Number Theory: Lang; Stewart & Tall; Frohlich & Taylor

Definition: An algebraic integer is the root of a monic polynomial in $\mathbb{Z}[x]$. An algebraic number is the root of a nonzero polynomial in $\mathbb{Z}[x]$.

A number field is a finite extension K of $\mathbb{Q}$ and we shall suppose it is in $\mathbb{C}$. Our object of study is the ring of algebraic integers in K.

Basic: Suppose L and K are finite extensions of $\mathbb{Q}$. L is an extension of K if $K \subset L$. The dimension of L over K in this case is $[L : K]$. Suppose next that H is a field with $K \subseteq H \subseteq L$. Then H is said to be an intermediate field of K and L. We have $[L : K] = [L : H][H : K]$.

A polynomial f in $K[x]$ is said to be irreducible if whenever $f = gh$ with g, $h \in K[x]$ then either g or h is a constant.

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

Definition: Let $K \subset \mathbb{C}$. Let $\theta \in \mathbb{C}$ be algebraic over K. A minimal polynomial f of θ over K is a monic polynomial in $K[x]$ which has θ as a root and has minimal degree with this property.

Theorem 1: Let $K \subseteq \mathbb{C}$. If $\theta \in \mathbb{C}$ is algebraic over K then θ has a unique minimal polynomial.
Proof: Suppose that $p_1(x)$ and $p_2(x)$ are minimal polynomials for θ over K. By the Division Algorithm for $K[x]$, $\exists c \in K$ and $r(x) \in K[x]$ such that $p_1(x) = cp_2(x) + r(x)$ with $r(x)$ the zero polynomial or $\deg r < \deg p_1 = \deg p_2$. But $p_1(\theta) = cp_2(\theta) + r(\theta)$ hence $r(\theta) = 0$. By the minimality of the degree we see that r is the zero polynomial.

Since p_1 and p_2 are monic we see that $c = 1$ hence $p_1 = p_2$ as required.

Definition: Suppose that θ is algebraic over K. Then the degree of θ over K is the degree of the minimal polynomial of θ over K.

Remark: Let θ be algebraic over K and let $p \in K[x]$ be the minimal polynomial of θ over K. If $f \in K[x]$ is a polynomial for which $f(\theta) = 0$ then $p \mid f$ in $K[x]$.

Theorem 2: Let $f \in K[x]$ with $K \subseteq \mathbb{C}$. If f is irreducible over K of degree n (≥ 1) then f has n distinct roots.
Proof: Suppose that f has a root α of multiplicity larger than 1. Then $f(x) = a_n(x - \alpha)^2 f_1(x)$ with $f_1 \in K(\alpha)[x]$. Thus

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

hence $f'(\alpha) = 0$ and note that $f' \in K[x]$. Let $p(x)$ be the minimal polynomial for α over K. Observe that $p(x)$ divides $f(x)$ and it divides $f'(x)$. Observe that $p(x)$ divides $f(x)$ and it divides $f'(x)$. Therefore f is reducible which is a contradiction.

Let θ be algebraic over K and let $p \in K[x]$ be the minimal polynomial of θ. Suppose that the degree of p is n. Then p has n distinct roots $\theta_1, \ldots, \theta_n$ and these are known as the conjugates of θ over K.

Definition: Let $K \subseteq \mathbb{C}$ and let θ be algebraic over K. $K(\theta)$ is defined to be the smallest field containing K and θ. $K(\theta)$ is said to be a simple algebraic extension of K.

PMATH 641 Lecture 2: January 11, 2013

If $K \subseteq \mathbb{C}$, θ is algebraic over K.

$$K(\theta) \coloneqq \text{smallest field containing } \theta \in K = \{\, f(\theta)/g(\theta) : f,\, g \in K[x] \text{ with } g(\theta) \neq 0 \,\}.$$

Theorem 3: Let $K \subset \mathbb{C}$, θ be algebraic over K. $\deg_k(\theta) = n$. Then every element $\alpha \in K(\theta)$ has a unique representation of the form:

$$\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$$

for $a_0, \ldots, a_{n-1} \in K$.
Proof: Since $\alpha \in K(\theta)$, $\alpha = f(\theta)/g(\theta)$. Let p be minimal polynomial of θ over K. Now $p(x)$ and $g(x)$ are coprime polynomials. There exists $s, t \in K[x]$ by Euclidean algorithm such that

$$p(x)t(x) + g(x)s(x) = 1$$

or $g(\theta)s(\theta) = 1 \implies \alpha = f(\theta)s(\theta)$. Now $f(x)s(x) = q(x)p(x) + r(x)$ by division so $f(\theta)s(\theta) = r(\theta)$, $\deg r(\theta) \leq n - 1$.
Proof of uniqueness:
$\alpha = r_1(\theta) = r_2(\theta)$; $r_1, r_2 \in K[x]$.
$r_1(x) - r_2(x)$ is polynomial of degree $< n$ having θ as root. This is not possible otherwise $\deg_k(\theta) \neq n$

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

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

Theorem 4: Let $K \subset \mathbb{C}$ and L be finite extensions of K. Each embedding of K in $\mathbb{C}$ extends to exactly $\deg_k(L)$ ($[L : K]$) embeddings of L in $\mathbb{C}$.
Proof: By induction on $[L : K]$.
Let $\alpha \in L \setminus K$, $p(x)$: minimal polynomial of α/K, let σ be an embedding of K in $\mathbb{C}$. $p(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{n} \sigma(a_i)x^i$ is irreducible over $\sigma(K)$.

For each root β of g, define an embedding λ_β of $K[\alpha]$ in $\mathbb{C}$ by $\lambda_\beta\colon K[\alpha] \to \mathbb{C}$,

$$\lambda_\beta(l_0 + l_1\alpha + \cdots + l_{n-1}\alpha^{n-1}) = \sigma(l_0) + \sigma(l_1)\beta + \cdots + \sigma(l_{n-1})\beta^{n-1}.$$

One can check λ_β is an embedding by checking it is an injective homomorphism and extends σ on K.

Further, there are no other embeddings since $\lambda(0) = 0 = p(\alpha) = \lambda p(\alpha) = g(\lambda_\alpha)$ (λ_α is a root of g)
Applying inductive hypothesis to $[L : K(\alpha)]$, there are exactly $[L : K(\alpha)][K(\alpha) : K]$ embeddings of L in $\mathbb{C}$.

PMATH 641 Lecture 3: January 14, 2013

Theorem 5: Let $K \subseteq L \subseteq \mathbb{C}$ and let L be a finite extension of K. Then $L = K(\theta)$ for some θ in L.
Proof: Note that

$$L = K(\gamma_1, \ldots, \gamma_n)$$

for some $\gamma_1, \ldots, \gamma_n$ algebraic over K. We'll now show our result by induction. It suffices to show that if $L = K(\alpha, \beta)$ with α, β algebraic over K then there exists $\theta \in L$ such that

$$L = K(\theta).$$

Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over K. Let $\beta = \beta_1, \ldots, \beta_m$ be the conjugates of β over K. Consider for each i and $k \neq 1$ the equation

$$\alpha_i + x\beta_k = \alpha_1 + x\beta_1.$$

There is precisely one solution. Now choose an element c in $K \setminus \{0\}$ which is not one of these solutions and put $\theta = \alpha + c\beta$.

We claim θ works. Notice that $K(\theta) \subseteq K(\alpha, \beta)$. To show that $K(\alpha, \beta) \subseteq K(\theta)$ it suffices to show that α and β are in $K(\theta)$. Observe that it suffices to show that β is in $K(\theta)$ since then automatically α is also in $K(\theta)$.

Let f be the minimal polynomial of α over K and let g be the minimal polynomial of β over K. Thus β is a root of $g(x)$ and also of $f(\theta - cx)$. Notice that $f(\theta - cx) \in K(\theta)[x]$. Further observe that β is the only common root of $g(x)$ and $f(\theta - cx)$, by our choice of c.

Let p be the minimal polynomial of β over $K(\theta)$. Then p divides g and p divides $f(\theta - cx)$. Therefore p is linear, in particular $\gamma_1\beta + \gamma_2 = 0$ with γ_1, $\gamma_2 \in K(\theta)$, $\gamma_1 \neq 0$ hence $\beta \in K(\theta)$.

Definition: Let $K \subseteq L \subseteq \mathbb{C}$ with $[L : K] < \infty$. We say that L is normal over K if L is closed under taking conjugates over K.

Theorem 6: Let $K \subseteq L \subseteq \mathbb{C}$ with $[L : K] < \infty$. L is normal over $K \iff$ Each embedding σ of L in $\mathbb{C}$ which fixes each element of K is an automorphism.
Proof: $\Rightarrow$ By Theorem 5 there exists a $\alpha \in L$ with $L = K[\alpha]$. Further let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over K. Then there are precisely n embeddings $\lambda_1, \ldots, \lambda_n$ of L in $\mathbb{C}$ which fix each element of K. We have $\lambda_i(\alpha) = \alpha_i$ for $i = 1, \ldots, n$.

Since L is normal $\lambda_i \colon L \to L$ for $i = 1, \ldots, n$. Next note $[K(\alpha_i) : K] = n$ for $i = 1, \ldots, n$ hence $L = K(\alpha_i)$ for $i = 1, \ldots, n$ and thus λ_i is an automorphism for $i = 1, \ldots, n$.

$\Leftarrow$ Let $\alpha \in L$ and let $\beta_1, \ldots, \beta_m$ be the conjugates of β over K.

Notice that each embedding of $K(\beta)$ in $\mathbb{C}$ which fixes elements of K can be extended to an embedding of L in $\mathbb{C}$ which fixes K. Each such embedding is an automorphism and so $\beta_i \in L$ for $i = 1, \ldots, m$ as required.

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

Theorem 7: Let $K \subseteq \mathbb{C}$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be algebraic over K. Put $L = K(\alpha_1, \ldots, \alpha_n)$. If L contains the conjugates of $\alpha_1, \ldots, \alpha_n$ over K then L is normal over K.
Proof: We have $K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$. Next by Theorem 5 there exists $\theta \in L$ such that $L = K[\theta]$. Then $\theta = f(\alpha_1, \ldots, \alpha_n)$ for some $f \in K[x_1, \ldots, x_n]$.

Let σ be an embedding of L in $\mathbb{C}$ which fixes K. Then $\sigma(\theta) = f(\sigma\alpha_1, \ldots, \sigma\alpha_n) \in L$. Therefore L is normal over K.

PMATH 641 Lecture 4: January 16, 2013

Corollary 8: Let $K \subseteq L \subseteq \mathbb{C}$ and let L be a finite extension of K. Then there is a finite extension H of L which is normal over K.
Proof: By Theorem 5, $L = K[\theta]$ where θ is algebraic over K. Let $\theta = \theta_1, \ldots, \theta_n$ be the conjugates of θ over K. We put $H = K(\theta_1, \ldots, \theta_n)$ and the result follows by Theorem 7.
Remark: H is normal over K and also normal over L.

Note that $\mathbb{Q}(\sqrt[3]{2})$ is not a normal extension of $\mathbb{Q}$ since $\omega\sqrt[3]{2}$ is a conjugate of $\sqrt[3]{2}$ over $\mathbb{Q}$ where $\omega = e^{2\pi i/3}$ and $\omega\sqrt[3]{2} \notin \mathbb{R}$ whereas $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Observe that by Corollary 8, $H = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ is normal over $\mathbb{Q}$. $H = \mathbb{Q}(\sqrt[3]{2}, \omega)$ so $[H : \mathbb{Q}(\sqrt[3]{2})] = 2$.

Let $K \subseteq L \subseteq \mathbb{C}$ with $[L : K] < \infty$. We define the Galois group $\mathrm{Gal}(L/K)$ to be the group of automorphisms of L which fixes each element of K. This is a group under the binary operation of composition. The identity element is the identity map. By Theorem 4 and Theorem 6

$$L \text{ is normal over } K \iff |\mathrm{Gal}(L/K)| = [L : K].$$

For each subgroup H of $G = \mathrm{Gal}(L/K)$ we define F_H to be the fixed field of H, in other words

$$F_H = \{\, \alpha \in L : \sigma\alpha = \alpha \text{ for all } \sigma \in H \,\}.$$

Note that F_H is a field.

Theorem 9: Let $K \subseteq L \subseteq \mathbb{C}$ with $[L : K] < \infty$. Suppose that L is normal over K and that G is the Galois group of L over K. Then K is the fixed field of G and K is not the fixed field of any proper subgroup H of G.
Proof: Plainly K is fixed by G. Suppose that there is an $\alpha \in L \setminus K$ which is fixed by G. Then $K[\alpha]$ is also fixed by G. By Theorem 4 and 6 there are exactly $[L : K[\alpha]]$ embeddings of L in $\mathbb{C}$ which fix $K[\alpha]$ and, since L is normal, each of them is an automorphism of L. Similarly, by Theorem 4 and 6, there are exactly $[L : K]$ embeddings of L in $\mathbb{C}$ which fix K and since L is normal each is an automorphism. But $[L : K[\alpha]] < [L : K]$ and this gives a contradiction.

We'll now suppose that K is the fixed field of a proper subgroup H of G. Let α be such that $L = K[\alpha]$ and define the polynomial f by

$$f(x) = \prod_{\sigma \in H} (x - \sigma\alpha).$$

Note that since H is a subgroup of G if $\sigma' \in H$ then $H\sigma' = \{\, \sigma\sigma' : \sigma \in H \,\} = H$. Therefore

$$f(x) = \prod_{\sigma \in H} (x - \sigma\sigma'\alpha).$$

Thus the coefficients of F are fixed by the elements of H. Thus $f \in K[x]$ with α as a root and it is monic. Therefore α is algebraic over K of degree at most $|H|$. But α is algebraic over K of degree $|G|$ since $L = K[\alpha]$ is normal over K. Finally since H is a proper subgroup of G, $|H| < |G|$ which gives a contradiction.

As always $K \subseteq L \subseteq \mathbb{C}$ with $[L : K] < \infty$. Suppose L is normal over K. Let $G = \mathrm{Gal}(L/K)$.
Let S_1 be the set of fields F with $L \subseteq F \subseteq K$.
Let S_2 be the set of subgroups H of G.

Define $\lambda\colon S_1 \to S_2$ by $\lambda(F) = \mathrm{Gal}(L/F)$. Define $\mu\colon S_2 \to S_1$ by $\mu(H) = F_H$ where F_H is the fixed field of H.

PMATH 641 Lecture 5: January 18, 2013

Let $K \subseteq L \subseteq \mathbb{C}$ with $[L : K] < \infty$. L normal over K. $G = \mathrm{Gal}(L/K)$ the Galois group of L over K. Recall the maps λ and μ, $\lambda\colon S_1 \to S_2$ by $\lambda(F) = \mathrm{Gal}(L/F)$, $\mu\colon S_2 \to S_1$ by $\mu(H) = F_H$, fixed field of H.

Theorem 10: (Fundamental Theorem of Galois Theory)
μ and λ are inverses of each other. Suppose that $\lambda(F) = H$. F is normal over K if and only if H is a normal subgroup of $G = \mathrm{Gal}(L/K)$. Further if F is normal over K there is an isomorphism δ of G/H to $\mathrm{Gal}(F/K)$ given by $\delta(\sigma + H) = \sigma|_F$; where $\sigma|_F$ is the automorphism of F which fixes each element of K given by the restriction of σ to F.
Proof: Note that

$$\mu \circ \lambda(F) = \mu(\mathrm{Gal}(L/F)) = F_{\mathrm{Gal}(L/F)}$$

By Theorem 9 the fixed field of $\mathrm{Gal}(L/F)$ is F and so $\mu \circ \lambda(F) = F$.

Further

$$\lambda \circ \mu(H) = \lambda(F_H) = \mathrm{Gal}(L/F_H).$$

Put $H' = \mathrm{Gal}(L/F_H)$. By Theorem 9, F_H is the fixed field of H' and of no proper subgroup of H'. Thus $H' \subseteq H$. But if $\sigma \in H$ then $\sigma \in \mathrm{Gal}(L/F_H)$ so $H \subseteq H'$. Thus $H = H'$ so $\lambda \circ \mu(H) = H$.

Suppose now $H = \mathrm{Gal}(L/F)$, $\gamma \in H$ and $\sigma \in G$. Then

$$\sigma \circ \gamma \circ \sigma^{-1} \text{ is in } \mathrm{Gal}(L/\sigma F)$$

Similarly if $\theta \in \mathrm{Gal}(L/\sigma F)$ then $\sigma^{-1}\theta\sigma$ is in $\mathrm{Gal}(L/F)$.

$$\implies \mathrm{Gal}(L/\sigma F) = \sigma H \sigma^{-1}.$$

Now if F is normal over K then $\sigma F = F$ for all σ in G.

F is normal over K and only every embedding of F in $\mathbb{C}$ which fixes K is an automorphism. Further every embedding of F in $\mathbb{C}$ which fixes K can be extended to an element of G.

$$\begin{aligned} F \text{ normal over } K &\iff \sigma F = F \,\forall \sigma \in G \\ &\iff \sigma H \sigma^{-1} = H \,\forall \sigma \in G \\ &\iff H \text{ is a normal subgroup of } G \end{aligned}$$

Next suppose F is normal over K. We introduce the group homomorphism in ψ from $G = \mathrm{Gal}(L/K)$ to $\mathrm{Gal}(F/K)$ given by

$$\psi(\sigma) = \sigma|_F,$$

where σ is the restriction of σ to F.

We first observe that the map is surjective since every element of $\mathrm{Gal}(F/K)$ can be extended to an element of G.

The kernel of ψ is $\mathrm{Gal}(L/F)$ so by the First Isomorphism Theorem

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \approx \mathrm{Gal}(F/K).$$

Theorem 11: Let α be an algebraic integer. The minimal polynomial of α over $\mathbb{Q}$ is in $\mathbb{Z}[x]$.
Proof: Let f be the minimal polynomial of α over $\mathbb{Q}$, $f \in \mathbb{Q}[x]$. Let h be a monic polynomial in $\mathbb{Z}[x]$ with α as a root. Since f is the minimal polynomial over $\mathbb{Q}$, $f \mid h$ is in $\mathbb{Q}[x]$. In particular there exist $g \in \mathbb{Q}[x]$ with $h = gf$.

Since h and f are monic we see that g is monic. By Gauss' Lemma there exist c_1, $c_2 \in \mathbb{Q}$ with

$$h = (c_1 g) \cdot (c_2 f),$$

where c_1 and c_2 are in $\mathbb{Q}$ and $c_1 g$ and $c_2 f$ are in $\mathbb{Z}[x]$. Note $c_1 = c_2 = 1$ since f and g are monic.

Corollary 12: Let d be a squarefree integer. The ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is

$$\{\, a + b\sqrt{d} : a, b \in \mathbb{Z} \,\} \text{ if } d \equiv 2, 3 \pmod 4$$

and

$$\left\{ \frac{a + b\sqrt{d}}{2} : a, b \in \mathbb{Z},\, a \equiv b \pmod 2 \right\} \text{ if } d \equiv 1 \pmod 4.$$

PMATH 641 Lecture 6: January 21, 2013

Corollary 12: Let d be a squarefree integer. The set of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is given by

$$\{\, a + b\sqrt{d} : a, b \in \mathbb{Z} \,\} \text{ if } d \equiv 2 \text{ or } 3 \pmod 4$$
$$\left\{ \frac{a + b\sqrt{d}}{2} : a, b \in \mathbb{Z} \right\} \text{ if } d \equiv 1 \pmod 4$$

Proof: Suppose that $\alpha \in \mathbb{Q}(\sqrt{d})$ then $\alpha = r + s\sqrt{d}$ with r, $s \in \mathbb{Q}$. Suppose that α is an algebraic integer.

First note that if $s = 0$ then $r \in \mathbb{Z}$. Suppose $s \neq 0$. Then observe that

$$f(x) = (x - (r + s\sqrt{d}))(x - (r - s\sqrt{d})) = x^2 - 2rx + (r^2 - ds^2)$$

is a monic polynomial over $\mathbb{Q}$ with α as a root. Since $\alpha \notin \mathbb{Q}$, f is the minimal polynomial of α. We need only check when $f \in \mathbb{Z}[x]$. Note that $2r \in \mathbb{Z}$ so either $r \in \mathbb{Z}$ or $r = a/2$ with $a \in \mathbb{Z}$ and $a \equiv 1 \pmod 2$. In the first case then $r^2 - ds^2 \in \mathbb{Z} \implies ds^2 \in \mathbb{Z}$. But d is squarefree and so $s \in \mathbb{Z}$.

In the second case $r = a/2$ and then

$$r^2 - ds^2 = a^2/4 - ds^2 \in \mathbb{Z} \implies s = b/2 \text{ with } b \equiv 1 \pmod 2$$

and then

$$\frac{a^2 - db^2}{4} \in \mathbb{Z} \implies d \equiv 1 \pmod 4$$

Objective: Prove

i) the set of all algebraic integers forms a ring.

ii) For any finite extension K of $\mathbb{Q}$ the set of algebraic integers in K, so $A \cap K$, forms a ring.

For any α, $\beta \in A$ we plan to show that $\alpha - \beta$ and $\alpha\beta$ are in A since this shows A is a subring of $\mathbb{C}$.

Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α. Let $\beta = \beta_1, \ldots, \beta_m$ be the conjugates of β.

Consider $\mathbb{Q}(\alpha, \beta)$. Let $\sigma_1, \ldots, \ldots_k$ be the embeddings of $\mathbb{Q}(\alpha, \beta)$ in $\mathbb{C}$ which fix $\mathbb{Q}$. Then put $g(x) = \prod_{i=1}^{k}(x - \sigma_i(\alpha - \beta))$. Note that g is monic. To prove $\alpha - \beta$ is an algebraic integer it suffices to prove $g \in \mathbb{Z}[x]$. This can be done using the elementary symmetric polynomials but there is an easier approach.

Theorem 13: Let $\alpha \in \mathbb{C}$. The following are equivalent:

i) α is an algebraic integer

ii) The additive subgroup of $\mathbb{Z}[\alpha]$ in $\mathbb{C}$ 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 of $\mathbb{C}$.

Proof: i) $\implies$ ii) by Theorem 3 since

$$\mathbb{Z}[\alpha] = \{\, a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_j \in \mathbb{Z} \,\}$$

where n is the degree of α over $\mathbb{Q}$.

ii) $\implies$ iii) $\implies$ iv) immediate

Finally suppose iv) is true. Since A is a finitely generated additive subgroup of $\mathbb{C}$ there exist $a_1, \ldots, a_n$ which generate A. Since $\alpha A \subseteq A$ we see that for $i = 1, \ldots, n$

$$\alpha a_i = m_{i,1}a_1 + \cdots + m_{i,n}a_n$$

with $m_{i,1}, \ldots, m_{i,n} \in \mathbb{Z}$. Put $M = (m_{i,j})$. Then

$$(\alpha I_n - M)\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Since $(a_1, \ldots, a_n) \neq (0, \ldots, 0) \implies \det(\alpha I_n - M) = 0 \implies \alpha$ is a root of a monic polynomial with coefficients in $\mathbb{Z}$, hence is an algebraic integer. Thus iv) $\implies$ i).

Corollary 14: If α and β are algebraic integers then so are $\alpha - \beta$ and $\alpha \cdot \beta$.
Proof: Suppose α has degree n over $\mathbb{Q}$ and β has degree m over $\mathbb{Q}$ then $\mathbb{Z}[\alpha, \beta]$ is generated over $\mathbb{Q}$ by

$\{\, \alpha^i\beta^j : i = 0, \dots, n-1,\, j = 0, \dots, m-1 \,\}$. Note $\alpha - \beta$ and $\alpha\beta$ are in the subring generated by this. The result follows by Theorem 13 ((i), (iii)).

Theorem 15: If α is an algebraic number then there exists a positive integer r such that $r\alpha$ is an algebraic integer.
Proof: Since α is an algebraic number it is the root of a polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ with $a_i \in \mathbb{Q}$. Clear denominators to get that α is a root of a polynomial

$$b_n x^n + \cdots + b_0 \text{ with } b_i \in \mathbb{Z}.$$

Then note $b_n\alpha$ is a root of

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0 b_n^{n-1}$$

and so $b_n\alpha$ is an algebraic integer.

PMATH 641 Lecture 7: January 23, 2013

Assignment #1: Due next Wednesday in class

$$\text{Corollary 14} \implies \text{The set } A \text{ of algebraic integers forms a subring of } \mathbb{C}.$$

Also if $[K : \mathbb{Q}] < \infty$ then $A \cap K$ is also a subring of $\mathbb{C}$. $A \cap K$ is the ring of algebraic integers of K.

Corollary 12 gives a description of $A \cap K$ when $[K : \mathbb{Q}] = 2$.

Next we'll consider the cyclotomic extensions of $\mathbb{Q}$. Let $n \in \mathbb{Z}^+$ and put $\zeta_n = e^{2\pi i/n}$. The fields $\mathbb{Q}(\zeta_n)$ for $n = 1, 2, \dots$ are significant. For instance they are normal extensions of $\mathbb{Q}$ with abelian Galois group. Further it can be shown that if L is a normal extension of $\mathbb{Q}$ with an abelian Galois group (over $\mathbb{Q}$) then L is a subfield of $\mathbb{Q}(\zeta_n)$.

Let $h(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and p be a prime. The map that sends h to $\overline{h} \in \mathbb{Z}/p\mathbb{Z}[x]$ where

$$\begin{aligned} \overline{h} &= \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_0} \\ \text{with } \overline{a_i} &= a_i + p\mathbb{Z} \end{aligned}$$

is a ring homomorphism. Further

$$\overline{h}(x^p) = (\overline{h}(x))^p \qquad \text{in} \qquad \mathbb{Z}/p\mathbb{Z}[x] \tag{$*$}$$

since

$$\begin{aligned} \overline{h}(x^p) &= \overline{a_n}x^{np} + \cdots + \overline{a_1}x^p + \overline{a_0} \\ &= \overline{a_n}^p x^{np} + \cdots + \overline{a_1}^p x^p + \overline{a_0}^p \\ &= (\overline{a_n}x^n + \cdots + \overline{a_0})^p \\ &= (\overline{h}(x))^p \end{aligned}$$

We now introduce $\Phi_n(x)$, the nth cyclotomic polynomial for $n = 1, 2, \dots$. We put

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

Theorem 16: $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$ for $n = 1, 2, \dots$.
Proof: We'll show that ζ_n^j for $1 \le j \le n$ with $(j,n) = 1$ are the conjugates of ζ_n and so $\Phi_n(x)$ is then the minimal polynomial of ζ_n. It is irreducible in $\mathbb{Q}[x]$.

Let $r(x)$ be the minimal polynomial of ζ_n. Since ζ_n is a root of $x^n - 1$, ζ_n is an algebraic integer. Note that then $r(x) \mid x^n - 1$ in $\mathbb{Q}(x)$ so $x^n - 1 = r(x)g(x)$ with $g(x) \in \mathbb{Q}[x]$. By Gauss' Lemma, $g \in \mathbb{Z}[x]$.

Since $r(x)$ divides $x^n - 1$ in $\mathbb{Q}[x]$ we see that the conjugates of ζ_n lie in

$$\{ \zeta_n^j : j = 1, \ldots, n \}.$$

Observe though that if $(j, n) > 1$ then $(\zeta_n^j)^{n/(j,n)} = 1$ whereas $(\zeta_n)^{n/(j,n)} \neq 1$ and so ζ_n^j is not a conjugate of ζ_n. In particular the conjugates of ζ_n lie in

$$\{ \zeta_n^j : j = 1, \ldots, n, \ (j, n) = 1 \}.$$

This is in fact the complete set of conjugates. To prove this it is enough to prove that if p is a prime which does not divide n and θ is a root of $r(x)$ then θ^p is also a root of $r(x)$. Note that ζ_n is a root of $r(x)$ and the result follows by repeated application of the above fact.

Recall that $x^n - 1 = r(x)g(x)$. Let θ be a root of $r(x)$. If θ^p is not a root of $r(x)$ then, since θ^p is a root of $x^n - 1$, we see that θ^p is a root of $g(x)$. Thus θ is a root of $g(x^p)$. Thus $r(x)$, the minimal polynomial of θ, divides $g(x^p)$ in $\mathbb{Q}[x]$ and so

$$g(x^p) = r(x)s(x) \qquad \text{with} \qquad s \in \mathbb{Q}[x].$$

By Gauss' Lemma $s(x) \in \mathbb{Z}[x]$.

Since $g(x^p) = r(x)s(x)$ we see that $\bar{r}(x) \mid \bar{g}(x^p)$ in $\mathbb{Z}/p\mathbb{Z}[x]$. Let t be an irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$ which divides $\bar{r}$. Now by $(*)$ t divides $\overline{g}(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$.

$$\begin{aligned} \text{Recall that } x^n - 1 &= r(x)g(x) \\ \text{so } x^n - \overline{1} &= \overline{r}(x)\overline{g}(x) \end{aligned}$$

Therefore $t^2 \mid x^n - \overline{1}$ in $\mathbb{Z}/p\mathbb{Z}[x]$, and so $t \mid \bar{n}x^{n-1}$. Since $p \nmid n$, $\bar{n}$ is not $\overline{0}$ hence $t = \overline{c}x^g$ with $1 \le g \le n - 1$. But $t \mid x^n - \overline{1}$ which gives a contradiction.

The result follows.

PMATH 641 Lecture 8: January 25, 2013

Midterm Exam: Friday March 1 in class

Observe that ζ_n^j is a conjugate of ζ_n for $j = 1, \ldots, n$ with $(j, n) = 1$. Certainly $\zeta_n^j \in \mathbb{Q}(\zeta_n)$ and so $\mathbb{Q}(\zeta_n)$ is a normal extension of $\mathbb{Q}$.

The degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$, Euler's function of n. In particular

$$\phi(n) = |\{ j : 1 \le j \le n, \ (j, n) = 1 \}|$$

Theorem 17: Let $n \in \mathbb{Z}^+$. The Galois group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.
Proof: The elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ fix $\mathbb{Q}$ and are determined by their action on ζ. In particular if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ then $\sigma(\zeta) = \zeta^k$ for some k with $1 \le k \le n$ and $(k, n) = 1$. Denote σ by σ_k.

Let $\lambda\colon \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ by $\lambda(\sigma_k) = k + n\mathbb{Z}$. Plainly λ is a bijection. It is also a group homomorphism since

$$\lambda(\sigma_k \circ \sigma_l) = \lambda(\sigma_{kl}) = kl + n\mathbb{Z} = (k + n\mathbb{Z}) \cdot (l + n\mathbb{Z}) = \lambda(\sigma_k) \cdot \lambda(\sigma_l).$$

Theorem 18: Let $n \in \mathbb{Z}^+$. 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 then $\mathbb{Q}(\zeta_n) = \mathbb{Q}(-\zeta_n) = \mathbb{Q}(\zeta_{2n})$. Thus to prove our result it suffices to prove it when n is even.

Suppose that $\gamma = e^{2\pi i l/s}$ with $(l, s) = 1$, e, $s \in \mathbb{Z}^+$. We consider $\gamma^v \zeta_n^w$ with v, $w \in \mathbb{Z}$ and note that $\gamma^v \zeta_n^w \in \mathbb{Q}(\zeta_n)$. Then

$$\begin{aligned}\gamma^v \zeta_n^w &= e^{2\pi i(\frac{vl}{s}+\frac{w}{n})} \\ &= e^{2\pi i(\frac{vln+sw}{ns})} \\ &= e^{2\pi i(\frac{1}{b})} \qquad \text{where } b = \frac{ns}{(n,s)} = \text{lcm}(n,s)\end{aligned}$$

Since $e^{2\pi i/b} \in \mathbb{Q}(\zeta_n)$ and degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$ we see that $\phi(b) \leq \phi(n)$.

Since $b = \text{lcm}(n, s)$ we have

$$b = p_1^{l_1} \cdots p_k^{l_k} \quad \text{with } p_i\text{s prime and } l_i \geq 1 \text{ for } i = 1, \ldots, k$$

Then, by reordering the primes,

$$n = p_1^{h_1} \cdots p_r^{h_r} \quad \text{with } r \text{ satisfying } 1 \leq r \leq k$$

and with $h_i \geq 1$ for $i = 1, \ldots, r$. Note $h_i \leq l_i$ for $i = 1, \ldots, r$. We have

$$\phi(b) = (p_1^{l_1} - p_1^{l_1-1}) \cdots (p_k^{l_k} - p_k^{l_k-1})$$

and

$$\phi(n) = \phi(p_1^{h_1}) \cdots \phi(p_r^{h_r}) = (p_1^{h_1} - p_1^{h_1-1}) \cdots (p_r^{h_r} - p_r^{h_r-1}).$$

But $\phi(b) \leq \phi(n)$.

If $r < k$ then $p_k \neq 2$ since n is even and $p_k^{l_k} - p_k^{l_{k-1}} > 1$ hence $\phi(b) > \phi(n)$ which is a contradiction. Therefore $r = k$. Since $l_i \geq h_i$ for $i = 1, \ldots, k$ we see that in fact $l_i = h_i$ for $i = 1, \ldots, k$ since $\phi(n) \geq \phi(b)$.

Let K be a finite extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] = n$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$.

Let $\alpha \in K$. We define the trace of α from K to $\mathbb{Q}$ denoted $T_{\mathbb{Q}}^K(\alpha)$, by

$$T_{\mathbb{Q}}^K(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha).$$

We define the norm of α from K to $\mathbb{Q}$, denoted by $N_{\mathbb{Q}}^K(\alpha)$, by

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

PMATH 641 Lecture 9: January 28, 2013

Let $[K : \mathbb{Q}] = n$ and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$. Let $\alpha \in K$. The trace of α from K to $\mathbb{Q}$, $T_{\mathbb{Q}}^K(\alpha)$ is given by $T_{\mathbb{Q}}^K(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$.

The norm $N_{\mathbb{Q}}^K(\alpha)$ is given by

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

Note $T_{\mathbb{Q}}^K$ is additive on K since for α, $\beta \in K$

$$T_{\mathbb{Q}}^K(\alpha + \beta) = T_{\mathbb{Q}}^K(\alpha) + T_{\mathbb{Q}}^K(\beta)$$

and also

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

Since the embeddings σ_i fix elements of $\mathbb{Q}$, for $r \in \mathbb{Q}$ we have

$$T_{\mathbb{Q}}^K(r\alpha) = \sigma_1(r\alpha) + \cdots + \sigma_n(r\alpha) = r(\sigma_1(\alpha) + \cdots + \sigma_n(\alpha)) = rT_{\mathbb{Q}}^K(\alpha)$$

and

$$N^K_{\mathbb{Q}}(r\alpha) = r^n N^K_{\mathbb{Q}}(\alpha).$$

Also note $\mathbb{Q}(\alpha)$ is contained in K so we can consider $N^{\mathbb{Q}(\alpha)}_{\mathbb{Q}}(\alpha)$ and $T^{\mathbb{Q}(\alpha)}_{\mathbb{Q}}(\alpha)$. These are coefficients in the minimal polynomial α.

$\implies N^{\mathbb{Q}(\alpha)}_{\mathbb{Q}}(\alpha)$ and $T^{\mathbb{Q}(\alpha)}_{\mathbb{Q}}(\alpha)$ are in $\mathbb{Q}$ and are in $\mathbb{Z}$ if α is an algebraic integer.

Theorem 19: Let K be a finite extension of $\mathbb{Q}$. Let $\alpha \in K$ and let $l = [K : \mathbb{Q}(\alpha)]$. Then

$$T^K_{\mathbb{Q}}(\alpha) = l T^{\mathbb{Q}(\alpha)}_{\mathbb{Q}}(\alpha)$$

and

$$N^K_{\mathbb{Q}}(\alpha) = (N^{\mathbb{Q}(\alpha)}_{\mathbb{Q}}(\alpha))^l.$$

Proof: Each of the embeddings of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ which fix $\mathbb{Q}$ extend to l distinct embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$ by Theorem 4. The result follows.

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

$$\alpha \text{ is a unit in } A \cap K \iff N^K_{\mathbb{Q}}(\alpha) = \pm 1.$$

Proof:

- $\Rightarrow$ Since α is a unit there is a $\beta \in A \cap K$ with $\alpha\beta = 1$. Thus $N^K_{\mathbb{Q}}(\alpha\beta) = N^K_{\mathbb{Q}}(1) = 1$. But $N^K_{\mathbb{Q}}(\alpha\beta) = N^K_{\mathbb{Q}}(\alpha)N^K_{\mathbb{Q}}(\beta)$ and since α, $\beta \in \mathbb{A} \cap K$ we see that $N^K_{\mathbb{Q}}(\alpha)$, $N^K_{\beta} \in \mathbb{Z}$. Hence $N^K_{\mathbb{Q}}(\alpha) = \pm 1$.
- $\Leftarrow$ Suppose $N^K_{\mathbb{Q}}(\alpha) = \pm 1$. Then let $\sigma_1(\alpha) = \alpha$, $\sigma_2(\alpha)$, $\ldots$, $\sigma_n(\alpha)$ be the images of σ_i.

  Thus

  $$\alpha((-1)^t \sigma_2(\alpha) \cdots \sigma_n(\alpha)) = 1$$

  where $t \in \{0, 1\}$. But $\beta = (-1)^t \sigma_2(\alpha) \cdots \sigma_n(\alpha)$ is in $\mathbb{A} \cap K$ since $\beta = \frac{1}{\alpha} \in K$ and $\sigma_i(\alpha)$ is an algebraic integer for $i = 2, \ldots, n$ hence $\beta \in \mathbb{A}$. Thus

  $$\beta \in \mathbb{A} \cap K.$$

Theorem 20 $\implies$ The set of units in $\mathbb{A} \cap K$ is a group under multiplication hence a subgroup of $\mathbb{C}$. What happens in $A \cap \mathbb{Q}(\sqrt{D})$ when D is a squarefree integer with $D \neq 1$?

What is the unit group?
If $D \not\equiv 1 \pmod 4$ then to determine the unit group we must find all elements $l + m\sqrt{D}$ with l, $m \in \mathbb{Z}$ for which

$$N^{\mathbb{Q}(\sqrt{D})}_{\mathbb{Q}}(l + m\sqrt{D}) = \pm 1 \tag{1}$$

hence for which $(l + m\sqrt{D})(l - m\sqrt{D}) = \pm 1 \implies l^2 - Dm^2 = \pm 1$. If $D \equiv 1 \pmod 4$ then we must also consider $\frac{l+m\sqrt{D}}{2}$ with l and m odd integers. Hence

$$N^{\mathbb{Q}(\sqrt{D})}_{\mathbb{Q}}\Big(\frac{l + m\sqrt{D}}{2}\Big) = \frac{l^2 - Dm^2}{4} = \pm 1 \implies l^2 - Dm^2 = \pm 4. \tag{2}$$

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 the units are ± 1, $\pm i$ or $D = -3$ in which case the units are ± 1, $\frac{\pm 1 \pm \sqrt{-3}}{2}$. Since D is negative we need only consider

$$l^2 - Dm^2 = +1 \text{ in (1)}$$

and

$$l^2 - Dm^2 = +4 \text{ in (2)}.$$

If $-D \neq 1$ or -3 then the only solution of (1) in integers l and m is given by $l = \pm 1$, $m = 0$. Similarly if $D \equiv 1 \pmod 4$ and $D \neq -3$ there are no solutions of (2) with l odd. If $D = -1$ then (1) has the solutions $l = \pm 1$, $m = 0$ and $l = 0$, $m = \pm 1$.

If $D = -3$ and l and m are odd then the solutions (l, m) are given by $(\pm 1, \pm 1)$. Further if $D = -3$ then (1) has only the solutions $l = \pm 1$, $m = 0$ in integers l, m.

Theorem 22: Let D be a squarefree integer larger than 1. There is a unit ϵ in $\mathbb{Q}(\sqrt{D})$ larger than 1 with the property that the group of units in $\mathbb{Q}(\sqrt{D})$ is

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

PMATH 641 Lecture 10: January 30, 2013

Given $\alpha \in \mathbb{R}$ how well can we approximate it with rationals p/q? How well can we approximate it in terms of q?

Dirichlet's Theorem: If $\alpha \notin \mathbb{Q}$ then

$$\text{there exists infinitely many } \frac{p}{q} \in \mathbb{Q} \text{ with } \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \qquad (*)$$

Lemma 23: Let α be a real *irrational* and let Q be an integer larger than 1. There exist integers p and q with $0 < p \leq Q$ such that $|p\alpha - q| < 1/Q$. Also we have $*$.

Proof: Note that $*$ follows from our first claim since

$$|q\alpha - p| < \frac{1}{Q} \implies \left|\alpha - \frac{p}{q}\right| < \frac{1}{pQ}$$

Thus if we pick a Q, we find $|\alpha - \frac{p_1}{q_1}| < \frac{1}{q_1 Q_1} \leq \frac{1}{q_1^2}$ with $q_1 \leq Q_1$. But then since α is irrational $\exists Q_2$ such that $\frac{1}{Q_2} < |q_1\alpha - p_1|$ and so $\exists \frac{p_2}{q_2} \neq \frac{p_1}{q_1}$ with $|\alpha - \frac{p_2}{q_2}| < \frac{1}{q_2^2}$. Continuing in this way we get our claim.

For any $x \in \mathbb{R}$ we define $\{x\}$, the fractional part of x to be $x - [x]$. We consider the $Q + 1$ number 0, 1, $\{\alpha\}$, $\{2\alpha\}$, $\ldots$, $\{(Q-1)\alpha\}$. Thus there exists an integer j with $1 \leq j \leq Q$ such that two of the numbers are in $\{\frac{j-1}{Q}, \frac{j}{Q}\}$ by the pigeonhole principle.

Note 0 and 1 are not both in the interval since $Q > 1$. Thus either there exist i_1 and i_2 with $\{i_1\alpha\}$, $\{i_2\alpha\}$ in $\left[\frac{j-1}{Q}, \frac{j}{Q}\right]$ with $1 \leq i_1 < i_2 \leq Q$ or there exist $t \in \{0, 1\}$ and i_1 with $1 \leq i_1 \leq Q$ with t and $\{i_1\alpha\}$ in $\left[\frac{j-1}{Q}, \frac{j}{Q}\right]$.

Then $|\{i_1\alpha\} - \{i_2\alpha\}| \leq 1/Q$ in the first case and $|t - \{i_1\alpha\}| \leq 1/Q$ in the second case. But $\{i_j\alpha\} = i_j\alpha - [i_j\alpha]$ for $j = 1$, 2. Thus in the first case $|\{i_1\alpha\} - \{i_2\alpha\}| = |(i_1 - i_2)\alpha - ([i_1\alpha] - [i_2\alpha])|$ and we take $q = i_1 - i_2$ and $p = [i_1\alpha] - [i_2\alpha]$. Since $\alpha \notin \mathbb{Q}$ we see that $|q\alpha - p| < 1/Q$ as required. The second case follows in a similar fashion.

Proof of Theorem 22: We'll first find a unit γ in $A \cap \mathbb{Q}(\sqrt{D})$ which is positive and different from 1. To show this we'll prove there exist a positive integer m and ∞-ly many $\beta \in A \cap \mathbb{Q}(\sqrt{D})$ for which $N_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{D})}(\beta) = N\beta = m$. Let $\beta = p + q\sqrt{D}$ with p, $q \in \mathbb{Z}$, $q \neq 0$. Then $N\beta = (p + q\sqrt{D})(p - q\sqrt{D}) = p^2 - Dq^2$. Then

$$|N\beta| = \left|\frac{p}{q} - \sqrt{D}\right| q^2 \left|\frac{p}{q} + \sqrt{D}\right|$$

We can find, by Dirichlet's Theorem, p, q with $|\frac{p}{q} - \sqrt{D}| < 1/q^2$ and then this implies $|\frac{p}{q} + \sqrt{D}| < 2\sqrt{D} + 1$ hence $|N\beta| < 2\sqrt{D} + 1$ for ∞-ly many pairs p, q with $(p, q) = 1$.

But $N\beta$ is an integer and so there is an integer m with $1 \leq |m| \leq 2\sqrt{D} + 1$ and ∞-ly many $\beta \in A \cap \mathbb{Q}(\sqrt{D})$ for which $N\beta = m$. We now choose an infinite subset of the βs so that if $\beta_1 = p_1 + q_1\sqrt{D}$ and $\beta_2 = p_2 + q_2\sqrt{D}$ are in the set then

$$p_1 \equiv p_2 \bmod m \text{ and}$$
$$q_1 \equiv q_2 \bmod m.$$

We now take from this subset β_1 and β_2 for which $\beta_1/\beta_2 \neq -1$ and consider β_1/β_2.

$$\frac{\beta_1}{\beta_2} = 1 + \frac{\beta_1 - \beta_2}{\beta_2} = 1 + \frac{(\beta_1 - \beta_2)\tilde{\beta}_2}{N\beta_2}$$

where $\tilde{\beta}_2$ is the conjugate of β_2. Thus

$$\frac{\beta_1}{\beta_2} = 1 + \Big(\frac{\beta_1 - \beta_2}{m}\Big)\tilde{\beta}_2 \in A \cap K.$$

Similarly $\beta_2/\beta_1 \in A \cap K$. Therefore β_1/β_2 is a unit in $A \cap \mathbb{Q}(\sqrt{D})$. It is not -1 by construction and so it is not a root of unity. Thus one of $\pm\beta_1/\beta_2$ is a positive unit different from 1. Thus there is a unit γ larger than 1.

PMATH 641 Lecture 11: February 1, 2013

Let

$$S = \{\, \gamma : \gamma \text{ a unit in } \mathbb{Q}(\sqrt{D}) \cap A \text{ with } \gamma > 0 \,\}.$$

We showed there exists an element γ_0 in S different from 1. By taking inverses if necessary we may suppose that $\gamma_0 > 1$.

But the elements of $A \cap \mathbb{Q}(\sqrt{D}) \cap \mathbb{R}^+$ are of the form $\frac{l+m\sqrt{D}}{2}$ with $l,\, m \in \mathbb{Z}$. Thus there are only finitely many elements of $A \cap \mathbb{Q}(\sqrt{D})$ larger than 1 and less than or equal to γ_0. Let ϵ be the smallest elements of S with $1 < \epsilon \leq \gamma_0$.

We claim $S = \{\, \epsilon^n : n \in \mathbb{Z} \,\}$.

Suppose that there is a unit λ in S which is not a power of ϵ. Then choose $n \in \mathbb{Z}$ such that

$$\epsilon^n < \lambda < \epsilon^{n+1}.$$

Consider $\lambda/\epsilon^n = \lambda(\epsilon^{-1})^n \in S$ since

$$N(\lambda(\epsilon^{-1})^n) = N(\lambda)(N(\epsilon^{-1}))^n = \pm 1.$$

But $1 < \lambda/\epsilon^n < \epsilon$ contradicting the minimality of ϵ. The result follows.

Theorem 24: Let K, L, M be finite extensions of $\mathbb{Q}$ with $K \subseteq L \subseteq M$. Let $\alpha \in M$ then $\mathrm{Tr}_K^M(\alpha) = \mathrm{Tr}_K^L(\mathrm{Tr}_L^M(\alpha))$ and $N_K^M(\alpha) = N_K^L(N_L^M(\alpha))$.

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.

If $\alpha \in M$ then

$$\mathrm{Tr}_K^L(\mathrm{Tr}_K^L(\alpha)) = \mathrm{Tr}_K^L(\tau_1(\alpha) + \cdots + \tau_m(\alpha)) = \sum_{i=1}^{n} \sigma_i(\tau_1(\alpha) + \cdots + \tau_m(\alpha)). \qquad (*)$$

Let N be a normal extension of M. We can extend $\sigma_1, \ldots, \sigma_n$ to embeddings of N in $\mathbb{C}$ which fix K, let us choose $\sigma_1', \ldots, \sigma_n'$. These are automorphisms of N which fix K. Let $\tau_1', \ldots, \tau_m'$ be embeddings of N in $\mathbb{C}$ which fix L.

We can compose σ_i' and τ_j' and we put $\sigma_i' \circ \tau_j'|_M$ to be the restriction of $\sigma_i' \circ \tau_j'$ to M. By $*$

$$\begin{aligned}
\mathrm{Tr}_K^L(\mathrm{Tr}_L^M(\alpha)) &= \sum_{i=1}^{n} \sigma_i'(\tau_1(\alpha) + \cdots + \tau_m'(\alpha)) \\
&= \sum_{i,j} \sigma_i' \circ \tau_j'(\alpha) \\
&= \sum_{i,j} \sigma_i' \circ \tau_j'|M(\alpha)
\end{aligned}$$

Notice that $\sigma_i' \circ \tau_j'|_M$ is an embedding of M in $\mathbb{C}$ which fixes K. If we can show that $\sigma_i' \circ \tau_j'|_M$ are distinct as we sum over i and j then they are the nm distinct embeddings of M in $\mathbb{C}$ which fix K and the result follows.

Suppose that $\sigma_i' \circ \sigma_j'|_M = \sigma_r' \circ \tau_s'|_M$. Next let γ be such that $L = K[\gamma]$.

$$\left.\begin{aligned} \text{Then } \sigma_i' \circ \tau_j'|_M(\gamma)^{1)} &= \sigma_i'(\gamma) = \sigma_i(\gamma) \\ \text{and } \sigma_r' \circ \tau_s|_M(\gamma) &= \sigma_r'(\gamma) = \sigma_r(\gamma) \end{aligned}\right\} i = r.$$

Next choose θ such that $M = L(\theta)$

$$\left.\begin{aligned} \sigma_i' \circ \tau_j'|_M(\theta)^{2)} &= \tau_j'(\theta) = \tau_j(\theta) \\ \sigma_i' \circ \tau_s'|_M(\theta) &= \tau_s'(\theta) = \tau_s(\theta) \end{aligned}\right\} j = s.$$

Similarly for the norm.

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 $\mathbb{Q}$. Let $\alpha_1, \ldots, \alpha_n$ be elements of K. We define the discriminant of the set $\{\alpha_1, \ldots, \alpha_n\}$, denoted by $\operatorname{disc}\{\alpha_1, \ldots, \alpha_n\}$, by

$$\operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} = (\det(\sigma_i(\alpha_j)))^2.$$

Note by properties of the determinant that the order in which we take the α_is or in which we take the σ_is does not matter.

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

$$\operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} = \det(\operatorname{Tr}_{\mathbb{Q}}^K(\alpha_i\alpha_j)).$$

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

$$(\sigma_j(\alpha_i))(\sigma_i(\alpha_j)) = (\operatorname{Tr}_{\mathbb{Q}}^K(\alpha_i\alpha_j)). \tag{$*$}$$

Thus

$$\begin{aligned} \operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} &= (\det(\sigma_i(\alpha_j)))^2 \\ &= \det(\sigma_j(\alpha_i)) \cdot \det(\sigma_i(\alpha_j)) \\ &= \det((\sigma_j(\alpha_i)) \cdot (\sigma_i(\alpha_j))) \\ &= \det(\operatorname{Tr}_{\mathbb{Q}}^K(\alpha_i\alpha_j)) \text{ by } *. \end{aligned}$$

Remark: Since $\mathrm{T}_{\mathbb{Q}}^K(\alpha_i\alpha_j) \in \mathbb{Q}$ we see that $\{\alpha_1, \ldots, \alpha_n\} \in \mathbb{Q}$. Further if $\alpha_1, \ldots, \alpha_n$ are in $A \cap K$ then $\alpha_i\alpha_j \in A \cap K$ and so $\mathrm{T}_{\mathbb{Q}}^K(\alpha_i\alpha_j) \in \mathbb{Z} \implies \operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} \in \mathbb{Z}$.

PMATH 641 Lecture 12: February 4, 2013

Let $[K : \mathbb{Q}] = n$. Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be bases for K (as a vector space over $\mathbb{Q}$). Write

$$\beta_k = \sum_{j=1}^n c_{kj}\alpha_j.$$

Then

$$(c_{kj}) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Since $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are bases we see that the matrix (c_{kj}) is invertible hence that $\det(c_{kj}) \neq 0$.

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

$$(c_{kj}) \begin{pmatrix} \sigma_t(\alpha_1) \\ \vdots \\ \sigma_t(\alpha_n) \end{pmatrix} = \begin{pmatrix} \sigma_t(\beta_1) \\ \vdots \\ \sigma_t(\beta_n) \end{pmatrix} \qquad \text{for } t = 1, \ldots, n.$$

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

$$(\det(c_{kj}))^2 \operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} = \operatorname{disc}\{\beta_1, \ldots, \beta_n\}. \tag{1}$$

Suppose that $K = \mathbb{Q}[\theta]$. Then $1, \theta, \ldots, \theta^{n-1}$ is a basis for K over $\mathbb{Q}$. Then

$$\begin{aligned} \operatorname{disc}\{1, \theta, \ldots, \theta^{n-1}\} &= \left(\det \begin{pmatrix} 1 & \sigma_1(\theta) & \cdots & \sigma_1(\theta^{n-1}) \\ \vdots & & & \\ 1 & \sigma_n(\theta) & \cdots & \sigma_n(\theta^{n-1}) \end{pmatrix} \right)^2 \\ &= \left(\det \begin{pmatrix} 1 & \sigma_1(\theta) & \cdots & (\sigma_1(\theta))^{n-1} \\ \vdots & & & \\ 1 & \sigma_n(\theta) & \cdots & (\sigma_n(\theta))^{n-1} \end{pmatrix} \right)^2 \\ &= \left(\prod_{1 \le i < j \le n} (\sigma_i(\theta) - \sigma_j(\theta)) \right)^2 \end{aligned}$$

But note that $\sigma_i(\theta) \neq \sigma_j(\theta)$ for $i \neq j$ hence $\operatorname{disc}\{1, \theta, \ldots, \theta^{n-1}\} \neq 0$.

Thus by (1) whenever $\alpha_1, \ldots, \alpha_n$ is a basis for K over $\mathbb{Q}$, $\operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} \neq 0$.

Remark: If $K \subseteq \mathbb{R}$ and K is normal over $\mathbb{Q}$ then by (1) whenever $\alpha_1, \ldots, \alpha_n$ is a basis for K over $\mathbb{Q}$ we see that

$$\operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} \in \mathbb{R}^+.$$

Theorem 27: Let $[K : \mathbb{Q}] = n$ and let $\alpha_1, \ldots, \alpha_n$ be in K.

$$\operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} = 0 \iff \alpha_1, \ldots, \alpha_n \text{ are linearly independent over } \mathbb{Q}.$$

Proof: $\Leftarrow$ Immediate from the definition of discriminant.
$\Rightarrow$ $\alpha_1, \ldots, \alpha_n$ is not a basis $\implies$ $\alpha_1, \ldots, \alpha_n$ are linearly dependent over $\mathbb{Q}$.

Note: The following is useful for computing the discriminant of $\{1, \theta, \ldots, \theta^{n-1}\}$ when $K = \mathbb{Q}(\theta)$. Let f be the minimal polynomial of θ over $\mathbb{Q}$. Then

$$\operatorname{disc}\{1, \theta, \ldots, \theta^{n-1}\} = (-1)^{n(n-1)/2} N_{\mathbb{Q}}^{K}(f'(\theta)).$$

To see this let $\theta = \theta_1, \ldots, \theta_n$ be the conjugates of θ. Then

$$f(x) = (x - \theta_1) \cdots (x - \theta_n)$$

and

$$f'(x) = \sum_{j=1}^{n} (x - \theta_1) \cdots \widehat{(x - \theta_j)} \cdots (x - \theta_n)$$

where $\widehat{(x - \theta_j)}$ means this term is removed from the product. Thus

$$f'(\theta_i) = (\theta_i - \theta_1) \cdots (\theta_i - \theta_n) \qquad \text{where } (\theta_i - \theta_i) \text{ is removed}$$

Further

$$N_{\mathbb{Q}}^{K}(f'(\theta)) = \prod_{i=1}^{n} \sigma_i(f'(\theta)) = \prod_{i=1}^{n} f'(\theta_i) = \prod_{i \neq j}(\theta_i - \theta_j)$$

Note that for $i \neq j$

$$(\theta_i - \theta_j) \cdot (\theta_j - \theta_i) = (-1) \cdot (\theta_i - \theta_j)^2$$

so

$$N_{\mathbb{Q}}^{K}(f'(\theta)) = (-1)^{n(n-1)/2} \left(\prod_{1 \leq i < j \leq n} (\theta_i - \theta_j) \right)^2$$

and our result follows.

Suppose $K = \mathbb{Q}[\theta]$, $[K : \mathbb{Q}] = n$. Then we abbreviate $\operatorname{disc}\{1, \theta, \ldots, \theta^{n-1}\}$ to $\operatorname{disc}(\theta)$.

Theorem 28: Let n be a positive integer. In $\mathbb{Q}(\zeta_n)$ we have that $\operatorname{disc}(\zeta_n)$ divides $n^{\phi(n)}$. Further if n is a prime we have

$$\operatorname{disc}(\zeta_n) = (-1)^{(p-1)/2} p^{p-2}.$$

Proof: We know that $\Phi_n(x)$ is the minimal polynomial for ζ_n. We have

$$\begin{aligned} & x^n - 1 = \Phi_n(x) \cdot g(x) \text{ with } g \in \mathbb{Z}[x]. \\ \Longrightarrow\ & nx^{n-1} = \Phi_n'(x) \cdot g(x) + \Phi_n(x) \cdot g'(x). \\ \Longrightarrow\ & n\zeta_n^{n-1} = \Phi_n'(\zeta_n) \cdot g(\zeta_n). \end{aligned}$$

Thus

$$\begin{aligned} N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(n) N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)} &= N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(\Phi_n'(\zeta_n)) \cdot N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(g(\zeta_n)) \\ n^{\phi(n)} &= ((-1)^{n(n-1)/2} \operatorname{disc}(\zeta_n)) \cdot N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(g(\zeta_n)) \in \mathbb{Z} \setminus \{0\}. \end{aligned}$$

PMATH 641 Lecture 13: February 6, 2013

Assignment #2 Typos: Q1(b) $2 \cdot 3$, Q3 $Q(\alpha) \to \mathbb{Q}(\theta)$.

Proof of Theorem 28

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(n) = N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(\zeta_n) N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(\Phi'(\zeta_n)) N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)} \tag{$*$}$$

where $x^n - 1 = \Phi_n(x) \cdot g(x)$ with $g \in \mathbb{Z}[x]$. Now take $n = p$, a prime in $*$.

$$\begin{aligned} N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(p) &= N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\zeta_p) N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\Phi_p'(\zeta_p)) N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(g(\zeta_p)) \\ p^{p-1} &= \zeta_p^{p(p-1)/2}(-1)^{(p-1)(p-2)/2} \operatorname{disc}(\zeta_p) N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(g(\zeta_p)) \\ p^{p-1} &= (-1)^{(p-1)/2} \operatorname{disc}(\zeta_p) \cdot N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(g(\zeta_p)) \end{aligned}$$

But $x^p - 1 = \Phi(x)(x-1)$ so $g(x) = x - 1$ and so

$$\begin{aligned} N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(g(\zeta_p)) &= N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\zeta_p - 1) \\ &= \prod_{j=1}^{p-1}(\zeta_p^j - 1) \\ &= \prod_{j=1}^{p-1}(1 - \zeta_p^j) \\ &= \Phi(1) \end{aligned}$$

and since $\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1}$ we see that $\Phi_p(1) = p$. Thus

$$\operatorname{disc}(\zeta_p) = (-1)^{(p-1)/2} \cdot p^{p-2}.$$

Definition: Let K be an extension of $\mathbb{Q}$ of degree n. A set of n algebraic integers $\{\alpha_1, \ldots, \alpha_n\}$ in K is said to be an integral basis for K if every algebraic integer in K can be uniquely expressed as an integral linear combination of $\alpha_1, \ldots, \alpha_n$.

Remarks: If $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis for K over $\mathbb{Q}$ then it is a basis for K over $\mathbb{Q}$. To see this note that if γ is in K then there is a positive integer r such that $r\gamma \in A \cap K$. But then since $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis there exist integers $a_1, \ldots, a_n$ such that

$$\begin{aligned} r\gamma &= a_1\alpha_1 + \cdots + a_n\alpha_n \\ \gamma &= \frac{a_1}{r}\alpha_1 + \cdots + \frac{a_n}{r}\alpha_n \end{aligned}$$

so γ is a $\mathbb{Q}$-linear combination of $\alpha_1, \ldots, \alpha_n$. Further $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$ and this follows since $[K : \mathbb{Q}] = n$.

Theorem 29: Let $[K : \mathbb{Q}] = n$. Then there exists an integral basis for K.
Proof: Consider the set of bases for K over $\mathbb{Q}$ which are made up of algebraic integers. The set is non-empty since there exists an algebraic integer θ such that $K = \mathbb{Q}[\theta]$. Then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis of algebraic integers.

Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for K comprised of algebraic integers for which $|\operatorname{disc}\{\alpha_1, \ldots, \alpha_n\}|$ is minimal. We claim that $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis for K. Suppose that it is not an integral basis. Then there exists an element γ in $\mathbb{A} \cap K$ which is not an integral linear combination of $\alpha_1, \ldots, \alpha_n$.

But $\{\alpha_1, \ldots, \alpha_n\}$ is a basis and so $\exists r_1, \ldots, r_n \in \mathbb{Q}$ with

$$\gamma = r_1\alpha_1 + \cdots + r_n\alpha_n.$$

By reordering we may suppose that $r_1 \notin \mathbb{Z}$. Put $b_1 = r_1 - \lfloor r_1 \rfloor$ and note $0 < b_1 < 1$. Note that $\gamma - \lfloor r_1 \rfloor \alpha_1 \in \mathbb{A} \cap K$ and

$$\gamma - \lfloor r_1 \rfloor \alpha_1 = b_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n.$$

Further observe that $\{\gamma - \lfloor r_1 \rfloor \alpha_1, \alpha_2, \ldots, \alpha_n\}$ is also a basis for K over $\mathbb{Q}$ consisting of algebraic integers. But

$$\begin{aligned} \operatorname{disc}\{\gamma - \lfloor r_1 \rfloor \alpha_1, \alpha_2, \ldots, \alpha_n\} &= \left(\det \begin{pmatrix} b_1 & r_2 & \ldots & r_n \\ & \ddots & 0 & \\ 0 & & 1 & \end{pmatrix} \right)^2 \operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} \\ &= b_1^2 |\operatorname{disc}\{\alpha_1, \ldots, \alpha_n\}| \end{aligned}$$

and since $0 < b_1^2 < 1$ we have a contradiction. The result follows.

Theorem 30: Let K be a finite extension of $\mathbb{Q}$. All integral bases for K have the same discriminant.
Proof: Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ be integral bases for K. Then

$$\alpha_j = \sum_{k=1}^{n} c_{jk}\beta_k \qquad \text{with } c_{jk} \in \mathbb{Z}.$$

Thus

$$\operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} = (\det(c_{jk}))^2 \operatorname{disc}\{\beta_1, \ldots, \beta_n\}.$$

Note $(\det(c_{jk}))^2 \in \mathbb{Z}^+$. Thus

$$\operatorname{disc}\{\beta_1, \ldots, \beta_n\} \mid \operatorname{disc}\{\alpha_1, \ldots, \alpha_n\}.$$

Similarly

$$\operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} \mid \operatorname{disc}\{\beta_1, \ldots, \beta_n\}.$$
$$\implies \operatorname{disc}\{\alpha_1, \ldots, \alpha_n\} = \pm\{\beta_1, \ldots, \beta_n\}$$

and since $(\det(c_{jk}))^2$ is positive the result follows.

PMATH 641 Lecture 14: February 11, 2013

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

How about quadratic extensions?

Let D be a squarefree non-zero integer. If $D \not\equiv 1 \pmod 4$ then 1, $\sqrt{D}$ is an integral basis for $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$.

$$\implies \operatorname{disc} \mathbb{Q}(\sqrt{D}) = \left(\det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}\right)^2 = 4D.$$

If $D \equiv 1 \pmod 4$ then 1, $(1+\sqrt{D})/2$ is an integral basis so

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

Next we'll show that if p is a prime then $\operatorname{disc}(\mathbb{Q}(\zeta_p)) = (-1)^{(p-1)/2} p^{p-2}$. This will follow provided we show that 1, ζ_p, …, ζ_p^{p-1} is an integral basis for $\mathbb{Q}(\zeta_p)$, i.e.,

$$A \cap \mathbb{Q}(\zeta_p) = \mathbb{Z}[\zeta_p].$$

More generally we'll show that if $n > 1$ that $A \cap \mathbb{Q}(\zeta_n) = \mathbb{Z}[\zeta_n]$, hence that 1, ζ_n, …, $\zeta_n^{\phi(n)-1}$ is an integral basis for $\mathbb{Q}(\zeta_n)$.

Theorem 31: Let K be a finite extension of $\mathbb{Q}$. Let α_1, …, α_n be a basis for K over $\mathbb{Q}$ consisting of algebraic integers. Let d be the discriminant of $\{\alpha_1, \ldots, \alpha_n\}$. Then if $\alpha \in \mathbb{A} \cap K$ there exist integers m_1, …, m_n with $d \mid m_i^2$ for $i = 1$, …, n such that

$$\alpha = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}.$$

Proof: Since α_1, …, α_n is a basis for K over $\mathbb{Q}$ there exist rationals a_1, …, a_n such that

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n.$$

Let σ_1, …, σ_n be the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$. Then

$$\sigma_j(\alpha) = a_1\sigma_j(\alpha_1) + \cdots + a_n\sigma_j(\alpha_n) \qquad \text{for } j = 1, \ldots, n.$$

Thus

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

By Cramer's rule

$$a_j = \frac{\det \begin{pmatrix} \sigma_1(\alpha) & \cdots & \sigma_1(\alpha)^{3)} & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots & & \vdots \\ \sigma_n(\alpha) & \cdots & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}}{\det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma(\alpha_1) \\ & \vdots & \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}}.$$

Since α and $\alpha_1, \ldots, \alpha_n$ are in $\mathbb{A} \cap K$ and $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ we see that

$$a_j = \frac{\gamma_j}{\delta} \qquad \text{where } \gamma_j \in \mathbb{A} \cap K$$

and where $\delta^2 = d$, for $j = 1, \ldots, n$.

Then

$$da_j = \delta\gamma_j \in \mathbb{A} \cap K \text{ for } j = 1, \ldots, n.$$

But $da_j \in \mathbb{Q}$ so da_j is an integer say m_j. It remains to show that $d \mid m_j^2$ for $j = 1, \ldots, n$. But

$$\frac{m_j^2}{d} = \frac{\delta^2\gamma_j^2}{d} = \gamma_j^2 \in \mathbb{A} \cap K \implies \frac{m_j^2}{d} \in \mathbb{Z} \implies d \mid m_j^2.$$

Let $[K : \mathbb{Q}] = n$ and let $K = \mathbb{Q}[\theta]$. Then for each embedding σ of K in $\mathbb{C}$ which fixes $\mathbb{Q}$ either $\sigma(\theta) \in \mathbb{R}$ or it is not. In the latter case there is another embedding $\overline{\sigma(\theta)}$ since $\mathbb{Q} \subseteq \mathbb{R}$. Therefore $n = r_1 + 2r_2$ where r_1 is the number of embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$ which embed K in $\mathbb{R}$ and $2r_2$ is the number of other embeddings.

Proposition 32: Let K be a finite extension of $\mathbb{Q}$ with r_1 real embeddings and $2r_2$ complex and not real embeddings. Then the sign of the dimension of K over $\mathbb{Q}$ is $(-1)^{r_2}$.
Proof: Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for K over $\mathbb{Q}$ and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$.

Then

$$\operatorname{disc}(K) = \left(\det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}\right)^2. \tag{$*$}$$

Note that

$$\overline{\det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}} = (-1)^{r_2} \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$$

since we are interchanging r_2 rows under complex conjugation. If r_2 is even then $\det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \in \mathbb{R}$ while if r_2 is odd then $\det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$ is purely imaginary. The result follows from $*$.

We'll first prove that if p is a prime and $r \in \mathbb{Z}^+$ then $\mathbb{A} \cap \mathbb{Q}(\zeta_{p^r}) = \mathbb{Z}[\zeta_{p^r}]$.

Note that

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

We have

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

$$\implies \Phi_{p^r}(1) = p \text{ hence } \prod_{j=1}^{p^r}(1 - \zeta_{p^r}^j) = p.$$

PMATH 641 Lecture 15: February 13, 2013

Recall that if p is a prime and $r \in \mathbb{Z}^+$ then

$$p = \prod_{\substack{j=1 \\ (j,p^r)=1}}^{p^r} (1 - \zeta_{p^r}^j).$$

Theorem 33: Let p be a prime and let $r \in \mathbb{Z}^+$. Then $\mathbb{A} \cap \mathbb{Q}(\zeta_{p^r}) = \mathbb{Z}[\zeta_{p^r}]$.
Proof: Note that $\mathbb{Q}(\zeta_{p^r}) = \mathbb{Q}(1 - \zeta_{p^r})$. Put $s = \phi(p^r)$. Then $1, 1 - \zeta_{p^r}, \ldots, (1 - \zeta_{p^r})^{s-1}$ is a basis for $\mathbb{Q}(\zeta_{p^r})$ over $\mathbb{Q}$ consisting of algebraic integers. By Theorem 31 if $\alpha \in \mathbb{A} \cap \mathbb{Q}(\zeta_{p^r})$ then there exist integers $m_0, \ldots, m_{s-1}$ such that

$$\alpha = \frac{m_0 + m_1(1 - \zeta_{p^r} + \cdots + m_{s-1}(1 - \zeta_{p^r})^{s-1})}{\operatorname{disc}(1 - \zeta_{p^r})}.$$

But

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

$$= \left(\prod_{\substack{1 \le i \le j \le p^r \\ (i,p)=1, (j,p)=1}} (\zeta_{p^r}^i - \zeta_{p^r}^j) \right)^2 = \operatorname{disc}(\zeta_{p^r}).$$

But $\operatorname{disc}(\zeta_{p^r})$ is a power of p and so we can write α in the form

$$\alpha = \frac{m_0 + m_1(1 - \zeta_{p^r}) + \cdots + m_{s-1}(1 - \zeta_{p^r})^{s-1}}{p^j} \qquad \text{for some integer } j.$$

Suppose $\mathbb{A} \cap \mathbb{Q}(\zeta_{p^r}) \neq \mathbb{Z}[1 - \zeta_{p^r}]$, in other words there exists an $\alpha \in \mathbb{A} \cap \mathbb{Q}(\zeta_{p^r})$ of the form

$$\alpha = \frac{l_0 + l_1(1 - \zeta_{p^r}) + \cdots + l_{s-1}(1 - \zeta_{p^r})^{s-1}}{p}$$

where $l_0, \ldots, l_{s-1}$ are integers not all divisible by p. Let i be the smallest integer for which $p \nmid l_i$. Then

$$\frac{l_i(1 - \zeta_{p^r})^i + \cdots + l_{s-1}(1 - \zeta_{p^r})^{s-1}}{p}$$

is in $\mathbb{A} \cap \mathbb{Q}(1 - \zeta_{p^r})$.

For every positive integer k, $1 - x$ divides $1 - x^k$ in $\mathbb{Z}[x]$. Recall that

$$p = \prod_{\substack{k=1 \\ (k,p)=1}}^{p^r} (1 - \zeta_{p^r}^k)$$

and so

$$p = (1 - \zeta_{p^r})^s \cdot \lambda \text{ where } \lambda \in \mathbb{A}.$$

Thus

$$(1 - \zeta_{p^r})^{s-(i+1)} \cdot \lambda \left(\frac{l_i(1 - \zeta_{p^r})^i + \cdots + l_{s-1}(1 - \zeta_{p^r})^{s-1}}{p} \right) \in \mathbb{A}$$

hence

$$\left(\frac{l_i(1 - \zeta_{p^r})^i + \cdots + l_{s-1}(1 - \zeta_{p^r})^{s-1}}{(1 - \zeta_{p^r})^{i+1}} \right) \in \mathbb{A}.$$

Thus $l_i/(1-\zeta_{p^r}) \in \mathbb{A}$ say is γ. But then $\gamma(1-\zeta_{p^r}) = l_i$ and hence

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{p^r})}(\gamma) \cdot N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{p^r})}(1-\zeta_{p^r}) = N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{p^r})}(l_i).$$

But then since $N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{p^r})}(1-\zeta_{p^r})$ is p we see that $p \mid l_i^s$ hence $p \mid l_i$ which is a contradiction. Thus $\mathbb{A} \cap \mathbb{Q}(\zeta_{p^r}) = \mathbb{Z}[1-\zeta_{p^r}]$ and since $\mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$ our result follows.

Let L and K be finite extensions of $\mathbb{Q}$. We denote by LK, the compositum of L and K the smallest field containing $L \cup K$.

Lemma 34: Let $[L:\mathbb{Q}] = m$ and $[K:\mathbb{Q}] = n$ and suppose $[LK:\mathbb{Q}] = mn$. Let σ be an embedding of L in $\mathbb{C}$ which fixes $\mathbb{Q}$ and let τ be an embedding of K in $\mathbb{C}$ which fixes $\mathbb{Q}$. Then there is an embedding of LK which when restricted to L is σ and when restricted to K is τ.
Proof: For each embedding σ of L we can consider the extensions of σ to embeddings of LK. There are n of them. Restricted to K there are n again. But there are exactly n embeddings of K and so one of them is τ.

Theorem 35: Let $[L:\mathbb{Q}] = m$, $[K:\mathbb{Q}] = n$ and $[LK:\mathbb{Q}] = mn$. Then

$$\mathbb{A} \cap LK \subseteq \frac{1}{d}(\mathbb{A} \cap K)(\mathbb{A} \cap L)$$

where $d = \gcd(\operatorname{disc}(K), \operatorname{disc}(L))$.
Proof: Ingredients: Lemma 34 and Cramer's Rule.

See Notes.

PMATH 641 Lecture 16: February 15, 2013

Theorem 36: Let $n \in \mathbb{Z}^+$. Then

$$\mathbb{A} \cap \mathbb{Q}(\zeta_n) = \mathbb{Z}[\zeta_n].$$

Proof: By induction on the number of prime factors of n. Result true for $n = 1$. If n has one prime factor the result follows from Theorem 33. Suppose now that

$$n = p_1^{l_1} \cdots p_k^{l_k}$$

with $l_i \in \mathbb{Z}^+$ and $p_1, \ldots, p_k$ distinct primes. By the inductive hypothesis

$$\mathbb{A} \cap \mathbb{Q}(\zeta_{p_1^{l_1} \cdots p_{k-1}^{l_{k-1}}}) = \mathbb{Z}[\zeta_{p_1^{l_1} \cdots p_{k-1}^{l_{k-1}}}]$$

and

$$\mathbb{A} \cap \mathbb{Q}(\zeta_{p_k^{l_k}}) = \mathbb{Z}[\zeta_{p_k^{l_k}}].$$

Note that the compositum of $\mathbb{Q}(\zeta_{p_1^{l_1} \cdots p_{k-1}^{l_{k-1}}})$ and $\mathbb{Q}(\zeta_{p_k^{l_k}})$ is $\mathbb{Q}(\zeta_n)$ since we can find integers g and h for which

$$\zeta^g_{p_1^{l_1} \cdots p_{k-1}^{l_{k-1}}} \cdot \zeta^h_{p_k^{l_k}} = \zeta_n.$$

By Theorem 23

$$\gcd(\operatorname{disc}(\mathbb{Q}(\zeta_{p_1^{l_1} \cdots p_{k-1}^{l_{k-1}}})), \operatorname{disc}(\mathbb{Q}(\zeta_{p_k^{l_k}}))) = 1.$$

We now apply Theorem 35 to conclude that

$$\mathbb{A} \cap \mathbb{Q}(\zeta_n) \subseteq \mathbb{A} \cap \mathbb{Q}(\zeta_{p_1^{l_1} \cdots p_{k-1}^{l_{k-1}}}) \cdot \mathbb{A} \cap \mathbb{Q}(\zeta_{p_k^{l_k}}).$$

But by (1) and (2)

$$\mathbb{A} \cap \mathbb{Q}(\zeta_{p_1^{l_1} \cdots p_{k-1}^{l_{k-1}}}) \cdot \mathbb{A} \cap \mathbb{Q}(\zeta_{p_k^{l_k}}) = \mathbb{Z}[\zeta_{p_1^{l_1} \cdots p_{k-1}^{l_{k-1}}}] \cdot \mathbb{Z}[\zeta_{p_k^{l_k}}]$$

which is

$$= \mathbb{Z}[\zeta_n] \implies \mathbb{A} \cap \mathbb{Q}(\zeta_n) = \mathbb{Z}[\zeta_n].$$

General problem: Given a finite extension K of $\mathbb{Q}$ how does one compute the discriminant of K? Find a θ which is an algebraic integer so that $K = \mathbb{Q}(\theta)$. Determine the discriminant of θ. If it is squarefree then it is the discriminant of K. We have seen that if $[K : \mathbb{Q}] = n$ then

$$\operatorname{disc}(\theta) = (-1)^{n(n-1)/2} N_{\mathbb{Q}}^{K}(f'(\theta))$$

where f is the minimal polynomial of θ over $\mathbb{Q}$. Suppose that f, $g \in \mathbb{C}[x]$ with

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

and

$$g(x) = b_m x^m + \cdots + b_1 x + b_0.$$

We define the resultant $R(f, g)$ by

$$\det \begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 \\ & a_n & a_{n-1} & \cdots & a_0 & & \\ & & \ddots & & & \ddots & \\ 0 & & & a_n & a_{n-1} & \cdots & a_0 \\ b_m & \cdots & \cdots & \cdots & b_0 & & 0 \\ & \ddots & & & & \ddots & \\ 0 & & b_m & \cdots & \cdots & \cdots & b_0 \end{pmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix} a \\ a \\ \ddots \\ a \end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix} b \\ \ddots \\ b \end{matrix}}\right\} n \text{ rows} \end{array}$$

Fact

(1) $R(f, g) = 0 \iff f$ and g have a common root.

(2) $\operatorname{disc}(\theta) = (-1)^{n(n-1)/2} R(f, f')$.

Example: Let $f(x) = x^3 - 5x + 1$. By Rational Roots Theorem since $f(1) \neq 1$, $f(-1) \neq 1$, we see that f is irreducible over $\mathbb{Q}$. Let θ be a root of f and put $K = \mathbb{Q}(\theta)$. What is $\operatorname{disc}(K)$?

First, what is $\operatorname{disc}(\theta)$? Thus

$$\begin{aligned} R(f, f') &= \det \begin{pmatrix} 1 & 0 & -5 & 1 & 0 \\ 0 & 1 & 0 & -5 & 1 \\ 3 & 0 & -5 & 0 & 0 \\ 0 & 3 & 0 & -5 & 0 \\ 0 & 0 & 3 & 0 & -5 \end{pmatrix} \\ &= \det \begin{pmatrix} 1 & 0 & -5 & 1 & 0 \\ 0 & 1 & 0 & -5 & 1 \\ 0 & 0 & 10 & -3 & 0 \\ 0 & 3 & 0 & -5 & 0 \\ 0 & 0 & 3 & 0 & -5 \end{pmatrix} \\ &= \det \begin{pmatrix} 1 & 0 & -5 & 1 \\ 0 & 10 & -3 & 0 \\ 0 & 0 & 10 & -3 \\ 0 & 3 & 0 & -5 \end{pmatrix} \\ &= \det \begin{pmatrix} 10 & -3 & 0 \\ 0 & 10 & -3 \\ 3 & 0 & -5 \end{pmatrix} \\ &= 10(-50) + 27 = -473 = -11 \cdot 43 \end{aligned}$$

By (2) we see that $\mathrm{disc}(\theta) = 473$. Since 473 is squarefree we see that

$$\mathrm{disc}(K) = 473.$$

Example: 2 Let $f(x) = x^3 + x^2 - 2x + 8$. Again f is irreducible over $\mathbb{Q}$ by Rational Roots Theorem. Let θ be a root of f and put $K = \mathbb{Q}(\theta)$. Further

$$R(f, f') = \det(\ ) = -4 \cdot 503.$$

We now try to modify the basis 1, θ, θ^2 in the hope of getting an integral basis. We can check that $(\theta + \theta^2)/2$ is an algebraic integer.

PMATH 641 Lecture 17: February 25, 2013

Recall: Let $f(x) = x^3 + x^2 - 2x + 8$ is irreducible over $\mathbb{Q}$. Let θ be a root of f. Put $K = \mathbb{Q}(\theta)$. We have $\mathrm{disc}(\theta) = -R(f, f') = -4 \cdot 503$.

Let $\theta = \theta_1$, θ_2, θ_3 be the conjugates of θ. We can check that

$$g(x) = \prod_{i=1}^{3} \Big(x - \frac{\theta_i^2 + \theta_i}{2}\Big)$$

is in $\mathbb{Z}[x]$. Thus $\frac{\theta^2+\theta}{2}$ is an algebraic integer. Then $\mathrm{disc}(1, \theta, \frac{\theta^2+\theta}{2}) = -503$. Thus 1, θ, $\frac{\theta^2+\theta}{2}$ is an integral basis for K since 503 is squarefree and $\mathrm{disc}(K) = -503$.

The question still remains: *is there* an integral power basis for K? In other words, is there $\lambda \in \mathbb{A} \cap K$ such that 1, λ, λ^2 is an integral basis?

Suppose we have such a λ. Then there exist integers a, b, and c so that

$$\lambda = a + b\theta + c\Big(\frac{\theta^2 + \theta}{2}\Big)$$

but then

$$\lambda^2 = A + B\theta + C\Big(\frac{\theta^2 + \theta}{2}\Big)$$

where $A = (a^2 - 2c^2 - 8bc)$, $B = (-2c^2 + 2ab + 2bc - b^2)$, and $C = (2b^2 + 2ac + c^2)$. Note

$$\begin{pmatrix} 1 \\ \lambda \\ \lambda^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ A & B & C \end{pmatrix} \begin{pmatrix} 1 \\ \theta \\ \frac{\theta^2+\theta}{2} \end{pmatrix}$$

so

$$\mathrm{disc}(\lambda) = \left(\det \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ A & B & C \end{pmatrix}\right)^2 \mathrm{disc}\Big(1, \theta, \frac{\theta^2 + \theta}{2}\Big) = \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ A & B & C \end{pmatrix} \cdot (-503).$$

But

$$\begin{aligned} \left(\det \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ A & B & C \end{pmatrix}\right)^2 &= (bC - Bc)^2 \\ &= (2b^3 - bc^2 + b^2c + 2c^3)^2 \\ &\equiv (b^2c - 2bc^2)^2 \bmod 2 \\ &\equiv (bc(b - c))^2 \bmod 2 \\ &\equiv 0 \bmod 2 \end{aligned}$$

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

$[K : \mathbb{Q}] < \infty$. An element α in $\mathbb{A} \cap K$ which is not zero and not a unit is said to be an irreducible of $\mathbb{A} \cap K$ if whenever $\alpha = \beta\gamma$ with β and γ in $\mathbb{A} \cap K$ then β is a unit or γ is a unit. We've seen that we don't have unique factorization into irreducibles up to units and reordering in $\mathbb{A} \cap \mathbb{Q}(\sqrt{-5})$. up to units and reordering in $\mathbb{A} \cap \mathbb{Q}(\sqrt{-5})$.

To recover unique factorization we pass to prime ideals in the ring.

Recall that an ideal P in a commutative ring with identity is a prime ideal $\iff$ whenever $ab \in P$ with a, $b \in R$ then $a \in P$ or $b \in P$. Also an integral domain is a commutative ring with identity with no zero divisors.

Suppose R is a subfield of a ring S. Then θ in S is said to be integral over R if it is the root of a monic polynomial with coefficients in R. R is integrally closed in S if whenever $\theta \in S$ is integral over R then $\theta \in R$.

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

(1) Every ideal in R is finitely generated.

(2) Every non-zero prime ideal in R is maximal

(3) R is integrally closed in its field of fractions.

Proposition 37: Let $[L : \mathbb{Q}] < \infty$. Let I be a non-zero ideal in $\mathbb{A} \cap K$. There is a positive integer in I.
Proof: Since I is non-zero there exists an $\alpha \in I$ with $\alpha \neq 0$. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over $\mathbb{Q}$. Then

$$N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = \alpha_1 \cdots \alpha_n = a \in \mathbb{Z} \setminus \{0\}.$$

Observe that $\alpha_2 \cdots \alpha_n = a/\alpha_1 \in K$. Further $\alpha_2, \ldots, \alpha_n$ are algebraic integers so $\alpha_2, \ldots, \alpha_n \in \mathbb{A}$. Thus $\alpha_2 \cdots \alpha_n \in \mathbb{A} \cap K$. Thus $(\alpha_1) \cdot (\alpha_2 \cdots \alpha_n) \in I$ so $a \in I$. But $-a \in I$ also.

Definition: Let $[K : \mathbb{Q}] < \infty$ and let I be a non-zero ideal in $\mathbb{A} \cap K$. Then $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis for the ideal if $\alpha_1, \ldots, \alpha_n$ are in I and every element of I has a unique representation as an integral linear combination of $\alpha_1, \ldots, \alpha_n$.

PMATH 641 Lecture 18: February 27, 2013

Midterm: Friday in class.

Theorem 38: Let $[K : \mathbb{Q}] < \infty$ and let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis for $\mathbb{A} \cap K$. Let I be a non-zero ideal in $\mathbb{A} \cap K$. Then there exists an integral basis $\{\alpha_1, \ldots, \alpha_n\}$ for I of the form

$$\begin{aligned}
\alpha_1 &= a_{11}\omega_1 \\
\alpha_2 &= a_{21}\omega_1 + a_{22}\omega_2 \\
&\vdots \\
\alpha_n &= a_{n1}\omega_1 + \cdots + a_{nn}\omega_n
\end{aligned}$$

where the $a_{ij} \in \mathbb{Z}$ and $a_{ii} \in \mathbb{Z}^+$ for $i = 1, \ldots, n$.
Proof: By Proposition 37 there exists a positive integer a in I. Thus $a\omega_i \in I$ for $i = 1, \ldots, n$. We choose α_1 to be the smallest positive multiple of ω_1 which is in I and denote it by $a_{11}\omega_1$. We then pick $\alpha_2, \alpha_3, \ldots$ by choosing α_i to be $a_{i1}\omega_1 + \cdots + a_{ii}\omega_i$ where α_i is the integer linear combination of $\omega_1, \ldots, \omega_i$ for which $a_{ii}\omega_i$ is such that a_{ii} is positive and minimal.

It remains to show that $\alpha_1, \ldots, \alpha_n$ is an integral basis for I. Since $\omega_1, \ldots, \omega_n$ are linearly independent over $\mathbb{Q}$ and $\det\begin{pmatrix} a_{11} & & 0 \\ \vdots & \ddots & \\ a_{n1} & & a_{nn} \end{pmatrix} \neq 0$ we see that $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$.

It remains to show that if $\beta \in I$ then β is an integral linear combination of $\alpha_1, \ldots, \alpha_n$. Since $\{\omega_1, \ldots, \omega_n\}$ is an integral basis for $\mathbb{A} \cap K$

$$\beta = b_1\omega_1 + \cdots + b_n\omega_n \text{ with } b_i \in \mathbb{Z}.$$

Notice that $a_{nn} \mid b_n$ since otherwise, by the Division Algorithm, we would contradict the minimality of a_{nn}. Thus $a_{nn} \cdot q_n = b_n$ for some integer q_n. But then $\beta - q_n\alpha_n$ is an integral linear combination of $\omega_1, \ldots, \omega_{n-1}$. We repeat the argument to find integers $q_1, \ldots, q_{n-1}$ so that

$$\beta = q_1\alpha_1 + \cdots + q_n\alpha_n$$

as required.

Theorem 39: Let $[K : \mathbb{Q}] < \infty$. Then $\mathbb{A} \cap K$ is a Dedekind Domain.
Proof: By Theorem 38 every ideal in $\mathbb{A} \cap K$ is finitely generated.

Let P be a non-zero prime ideal in $\mathbb{A} \cap K$. We'll show that P is maximal.

First note that there is a positive integer a in P. Next note that since P is a prime ideal $\mathbb{A} \cap K/P$ is an integral domain.

Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis for $\mathbb{A} \cap K$. Then $\mathbb{A} \cap K/P$ is made up of cosets of the form

$$a_1\omega_1 + \cdots + a_n\omega_n + P$$

where the a_is are integers of size at most a in absolute value. $\implies$ $\mathbb{A} \cap K/p$ is finite.

But a finite integral domain is a field and so P is maximal.

Finally, let $\gamma = \frac{\alpha}{\beta}$ with α, $\beta \in \mathbb{A} \cap K$, $\beta \neq 0$. Suppose that γ is integral over $\mathbb{A} \cap K$. Thus γ is the root of a polynomial $x^m + \alpha_{m-1}x^{m-1} + \cdots + \alpha_0$ with $\alpha_{m-1}, \ldots, \alpha_0$ in $\mathbb{A} \cap K$ $(*)$. It remains to show that $\gamma \in \mathbb{A} \cap K$. Plainly $\gamma \in K$. It remains to show that $\gamma \in \mathbb{A}$.

We do so by considering the ring

$$S = \mathbb{Z}[\alpha_0, \ldots, \alpha_{n-1}, \gamma].$$

Plainly $\gamma \in S$. By Theorem 13 it suffices to show that S is finitely generated as an additive group. Let $\theta \in S$ then it is enough to show that θ is an integral linear combination of terms of the form

$$\alpha_0^{b_0} \cdots \alpha_{m-1}^{b_{m-1}} \gamma^{b_m}$$

where $b_m < m$ and the b_is for $i = 0, \ldots, m-1$ are less than n.

It is enough to show that if θ is of the form $\alpha_0^{c_0} \cdots \alpha_{m-1}^{c_{m-1}} \gamma^{c_m}$ with $c_0, \ldots, c_m \in \mathbb{Z}_{\geq 0}$ then this is true.

Start by using $*$, in other words

$$\gamma^m = -\alpha_{m-1}\gamma^{m-1} \cdots - \alpha_0,$$

to reduce c_m to an integer of size at most $m - 1$.

PMATH 641 Lecture 19: March 4, 2013

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 non-empty set of ideals in R has a maximal element.

Proof: (1) $\implies$ (2). Suppose that $I_1 \subseteq I_2 \subseteq \cdots$ with $I_i \in R$ for $i = 1, 2, \ldots$. Put

$$I = \bigcup_{n=1}^{\infty} I_n.$$

Then I is an ideal of R and so $I = (\alpha_1, \ldots, \alpha_t)$. But notice that α_j is in I so there exists an integer n_j so that $\alpha_j \in I_{n_j}$ for $j = 1, \ldots, t$. But then $I \subseteq I_b$ where $b = \max(n_1, \ldots, n_t)$. Thus $I = I_b = I_{b+1} = \cdots$.

(2) $\implies$ (3). Let S be a non-empty set of ideals in R. Thus there exists I_1 in S. Either I_1 is maximal in S or there exists I_2 in S with $I_1 \subsetneq I_2$. Either I_2 is maximal in S or there exists I_3 in S with $I_2 \subsetneq I_3$. Eventually this process terminates by (2).

(3) $\implies$ (1). Let I be an ideal of R. Let S be the set of finitely generated ideals of R in I. (0) is in I so S is non-empty. Let M be a maximal element of S. Then $M \subseteq I$. Suppose that $M \subsetneq I$.

Now M is finitely generated so $M = (\alpha_1, \ldots, \alpha_t)$ say. Pick $\gamma \in I \setminus M$. Then the ideal $I_1 = (\alpha_1, \ldots, \alpha_t, \gamma)$ is in I and so M is not a maximal element of S which is a contradiction. Thus $M = I$. ✓

Lemma 41: In a Dedekind domain every non-zero ideal contains a product of non-zero prime ideals. (Here the product may be a product of 1 element.)
Proof: Let S be the set of non-zero ideals in the Dedekind domain R which do not contain a product of non-zero prime ideals. Suppose that S is non-empty. Then by the definition of a Dedekind domain and Theorem 40 we see that S has a maximal element M. Note that M is not a prime ideal. Thus there exist a, $b \in R$ with $ab \in M$ and $a \notin M$, $b \notin M$. Therefore

$$(M + (a))(M + (b)) \subseteq M.$$

But $M \subsetneq M + (a)$ and $M \subsetneq M + (b)$. Since M is maximal both $M + (a)$ and $M + (b)$ contain a product of non-zero prime ideals. Then by $*$ so does M which is a contradiction.

Lemma 42: Let I be a prime ideal in a Dedekind domain R with field of fractions K. Then there is an element $\gamma \in K \setminus R$ such that $\gamma I \subseteq R$.
Proof: Let a be any non-zero element of I. Then $\frac{1}{a} \notin R$ since I is proper.

PMATH 641 Lecture 20: March 6, 2013

Lemma 42: Let I be a proper ideal in a Dedekind domain R with field of fractions K. There is an element γ in $K \setminus R$ for which

$$\gamma I \subseteq R.$$

Proof: Let a be a non-zero element in I. Since I is proper a is not a unit and so $\frac{1}{a} \in K \setminus R$. (a) contains a product of prime ideals $p_1 \cdots p_r$ by Lemma 41. Let us suppose that r is minimal.

Let S be the set of proper ideals in R which contains I. S is non-empty and so by Theorem 40, S contains a maximal element M. Observe that M is a maximal ideal. Since R is a Dedekind domain, M is a prime ideal. Next note that $(a) \subseteq I$ and also $p_1 \cdots p_r \subseteq (a) \subseteq I \subseteq M$.

We claim that $M \supseteq p_i$ for some i with $1 \leq i \leq r$. Suppose not. Then there is an element a_i in p_i and not in M for $i = 1, \ldots, r$. But then $a_1 \cdots a_r \in M$ with $a_i \notin M$ for $i = 1, \ldots, r$ contradicting the fact that M is a prime ideal. Thus $M \supseteq p_i$ for some i. Without loss of generality we may suppose $M \supseteq p_1$. Since M is a prime ideal $M = p_1$.

Recall $(a) \supseteq p_1 \cdots p_r$ with r minimal. If $r = 1$ then $p_1 \subseteq (a) \subseteq I \subseteq M$ so $p_1 = (a)$ and then with $\gamma = \frac{1}{a}$ we have

$$\gamma I = \frac{1}{a}(a) = R$$

as required.

If $r > 1$ then we consider $p_2 \cdots p_r$. Note that $p_2 \cdots p_r$ is non-empty and not contained in (a). Thus there exists an element b in $p_2 \cdots p_r$ which is not in (a). We now take $\gamma = \frac{b}{a}$. Observe that $\gamma \in K \setminus R$.

Then

$$\begin{aligned}\gamma I &= \frac{b}{a} I \\ &\subseteq \frac{b}{a} p_1 \\ &\subseteq \frac{(b)p_1}{a} \\ &\subseteq \frac{1}{a} p_1 \cdots p_r \\ &\subseteq \frac{1}{a}(a) \\ &= R,\end{aligned}$$

as required.

Theorem 43: Let R be a Dedekind domain and let I be an ideal of R. Then there is an ideal J of R for which

$$IJ \text{ is a principal ideal of } R.$$

Proof: If $I = (0)$ the result is immediate so suppose that I is not (0). Let α be a non-zero element of I.

Define J to be the following set in R:

$$J = \{\, \beta \in R : \beta I \subseteq (\alpha) \,\}.$$

Note that J is an ideal of R and

$$IJ \subseteq (\alpha).$$

We want to show that in fact $IJ = (\alpha)$. Put $B = \frac{1}{\alpha} IJ$ and note B is an ideal of R. If $B = R$ we are done since then $IJ = (\alpha)$.

Suppose then that B is a proper ideal of R. Then by Lemma 42 there exists a $\gamma \in K \setminus R$ for which $\gamma B \subseteq R$; here K is the field of fractions of R. Since $\alpha \in I$ we have that $J \subseteq \frac{1}{\alpha} IJ = B$. Thus

$$\gamma J \subseteq \gamma B \subseteq R.$$

Thus $\gamma JI \subseteq (\alpha)$ and so by the definition of J, $\gamma J \subseteq J$. But J is a finitely generated additive subgroup of the field of fractions of the Dedekind domain R.

By Theorem 13 with $\mathbb{C}$ replaced by the field of fractions of a Dedekind domain we see that γ is the root of a monic polynomial with coefficients in R. Since R is a Dedekind domain it is integrally closed in its field of fractions. Thus $\gamma \in R$ which is a contradiction.

PMATH 641 Lecture 21: March 8, 2013

Theorem 43

$$\vdots$$

$$\gamma J \subset J$$

J is a finitely generated ideal in R so $J = (a_1, \ldots, a_n)$.

Then there exist m_{ij} in R so that

$$\gamma a_i = m_{i1} a_1 + \cdots + m_{in} a_n$$

for $i = 1, \ldots, n$. Then

$$(\gamma I_n - M)\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

where $M = (m_{ij})$. $J \neq (0)$ so $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \implies \det(\gamma I_n - M) = 0$. Thus γ is the root of a monic polynomial with entries in R. But R is a Dedekind domain so R is integrally closed in its field of fractions K. Since $\gamma \in K$ we see that $\gamma \in R$. This is a contradiction.

Corollary 44: Let A, B and C be non-zero ideals in a Dedekind domain R with $AC = BC$ then $A = B$.
Proof: There exists an ideal J in R so that CJ is principal. Say $CJ = (\alpha)$ with $\alpha \in R$. Note that

$$ACJ = BCJ$$

so $A(\alpha) = B(\alpha)$.

$$\implies A\alpha = B\alpha$$

$\implies A = B$ since $\alpha \neq 0$.

Corollary 45: Let A and B be non-zero ideal in a Dedekind domain R.

$$A \mid B \iff B \subseteq A.$$

Proof: $\Rightarrow$ Since $A \mid B$ there exists an ideal C in R with $AC = B$. Then immediately $B \subseteq A$.
$\Leftarrow$ By Theorem 43 there exists a non-zero element α in R and an ideal J of R such that $AJ = (\alpha)$. Consider $\frac{1}{\alpha}BJ$. Note that $\frac{1}{\alpha}BJ$ is an ideal of R since $B \subseteq A$. Further $A(\frac{1}{\alpha}BJ) = B(\frac{1}{\alpha}AJ) = B(\frac{1}{\alpha}(\alpha)) = B$.

Theorem 46: Every non-zero proper ideal in a Dedekind domain R can be written as a product of prime ideals of R and this representation as a product is unique up to ordering.
Proof: We first prove existence.

Let S be the set of non-zero proper ideals which cannot be written as a product of prime ideals. Since R is a Dedekind domain S has a maximal element M. Note that M is contained in a maximal ideal of R which, since R is a Dedekind domain, is a prime ideal of R, say P.

Thus $M \subseteq P$. Note $M \neq P$ since M is in S. Thus $M \subsetneq P$. Therefore by Corollary 45 there exists an ideal A such that

$$M = PA.$$

Further $M \subsetneq A$. But A is not a product of prime ideals since otherwise by $*$ M is a product of prime ideals. But then $A \in S$ and M is not maximal in S which is a contradiction. Therefore S is empty as required.

"Uniqueness"
Suppose that $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ are prime ideals with

$$p_1 \cdots {}_r = q_1 \cdots q_s.$$

Note that $p_1 \mid q_1 \cdots q_s$. Thus by Corollary 45, $p_1 \supseteq q_1 \cdots q_s$. Since p_1 is a prime ideal $p_1 \supseteq q_i$ for some i. Without loss of generality we may suppose $p_1 \supseteq q_1$. Prime ideals are maximal ideals in R so $p_1 = q_1$. By Corollary 44, $p_2 \cdots p_r = q_2 \cdots q_s$. Repeating this argument the result follows.

Remark: Let $[K : \mathbb{Q}] < \infty$. Then $\mathbb{A} \cap K$ is a Dedekind domain and so we have unique factorization into prime ideals, up to ordering, in $\mathbb{A} \cap K$.

Definition: Let R be a commutative ring with identity. An element c of R is said to be irreducible of R if

(1) $c \neq 0$ and c is not a unit of R.

(2) If $c = ab$ with a, b in R then a is a unit or b is a unit.

An element c of R is said to be a prime of R if

(1) $c \neq 0$ and c is not a unit of R

(2) If $c \mid ab$ with a, b in R then $c \mid a$ or $c \mid b$.

Note in UFDs the concepts are the same.

PMATH 641 Lecture 22: March 11, 2013

Theorem 47: Let $[K : \mathbb{Q}] < \infty$. The factorization of elements of $\mathbb{A} \cap K$ into irreducibles is unique up to reordering and units if and only if every ideal in $\mathbb{A} \cap K$ is principal.
Proof: $\Leftarrow$ It is enough to show that every non-zero prime ideal P in $\mathbb{A} \cap K$ is principal. By Proposition 37 there is an integer a with $a > 1$ in P. Let $a = \pi_1 \cdots \pi_t$ be the decomposition of a into irreducibles in $\mathbb{A} \cap K$.

Then $a \in P$ so $P \supseteq (a) = (\pi_1) \cdots (\pi_t)$. Thus $P \mid (\pi_1) \cdots (\pi_t)$ so $P \mid (\pi_i)$ for some i with $1 \leq i \leq t$. Without loss of generality we may suppose that $P \mid (\pi_1)$ so $P \supseteq (\pi_1)$.

Notice that $P = (\pi_1)$ since (π_1) is a prime ideal. This follows since otherwise $(\pi_1)\delta = \beta\gamma$ with β and γ not in (π_1). But π_1 is irreducible so $\pi_1 \mid \beta$ or $\pi_1 \mid \gamma$ by unique factorization which is a contradiction.

$\Rightarrow$ Suppose that

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

where the π_i and λ_j are irreducibles in $\mathbb{A} \cap K$. Notice that then

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

Therefore it suffices to show that if π is an irreducible of $\mathbb{A} \cap K$ then (π) is a prime ideal. We have unique factorization into prime ideals of $\mathbb{A} \cap K$ so if (π) is not a prime ideal then $(\pi) = AB$ with A and B proper non-zero ideals of $\mathbb{A} \cap K$.

Since every ideal in $\mathbb{A} \cap K$ is principal there exists $\alpha, \beta \in \mathbb{A} \cap K$ with $A = (\alpha)$ and $B = (\beta)$. Then $(\pi) = (\alpha)(\beta)$. Thus there exists $\delta, \gamma \in \mathbb{A} \cap K$ such that $\pi = \{\alpha\delta\} \cdot \{\beta\gamma\}$. But π is irreducible so either $\alpha\delta$ is a unit in which case α is a unit or $\beta\gamma$ is a unit in which case β is a unit. This contradicts the fact that A and B are proper ideals.

The only rings $\mathbb{A} \cap \mathbb{Q}(\sqrt{-D})$ which have unique factorization into irreducibles with $D > 0$ are those with

$$D = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

Given a prime ideal P in $\mathbb{A} \cap K$ with $[K : \mathbb{Q}] < \infty$ we can find an integer $a > 1$ with $a \in P$. Let $a = p_1 \cdots p_t$ be a factorization of a into primes in $\mathbb{Z}$. Then $P \supseteq (a)$ so $P \mid (p_1) \cdots (p_t)$ hence $P \mid (p_i)$ for some prime p_i in $\mathbb{Z}$.

Suppose $P \mid (p)$ are $P \mid (q)$ for two distinct primes p, q in $\mathbb{Z}$. Then since there exist integers r and s with

$$rp + sq = 1$$

we see that

$$(r)(p) + (s)(q) = (1)$$

and so

$$P \mid (1)$$

which is a contradiction. Thus to each prime ideal P in $\mathbb{A} \cap K$ there is a unique prime p in $\mathbb{Z}$ associated to it with $P \mid (p)$.

Definition: Let $[K : \mathbb{Q}] < \infty$ and let p be a prime in $\mathbb{Z}$. We say that p ramifies in $\mathbb{A} \cap K$ if there exists a prime ideal P in $\mathbb{A} \cap K$ such that $P^2 \mid (p)$.

Dedekind proved that the primes p that ramify are exactly the primes that divide the discriminant D.

PMATH 641 Lecture 23: March 13, 2013

Theorem 48: Let $[K : \mathbb{Q}] < \infty$. Let D be the discriminant of K. If p is a prime which does not divide D then p is unramified in $\mathbb{A} \cap K$.
Proof: We'll prove the contrapositive.

Suppose that P is a prime ideal and $P^2 \mid (p)$. We'll show that then $p \mid D$.

Since $P^2 \mid (p)$ there is an ideal Q with $P^2 Q = (p)$. Then there exists an $\alpha \in \mathbb{A} \cap K$ with $\alpha \in PQ$ but $\alpha \notin P^2 Q$.

But then $\alpha^2 \in P^2 Q^2$ and so $\alpha^2 \in (p)$ hence $\alpha^2/p \in \mathbb{A} \cap K$. Thus $\alpha^p/p \in \mathbb{A} \cap K$ and so for each $\beta \in \mathbb{A} \cap K$, $(\alpha\beta)^p/p \in \mathbb{A} \cap K$. Notice then that $T_{\mathbb{Q}}^K(\alpha\beta)^p = T_{\mathbb{Q}}^K(p(\alpha\beta)^p/p) = pT_{\mathbb{Q}}^K((\alpha\beta)^p/p)$. Since $T_{\mathbb{Q}}^K((\alpha\beta)^p/p)$ is an integer we see that $p \mid T_{\mathbb{Q}}^K(\alpha\beta)^p$. But

$$(T_{\mathbb{Q}}^K \alpha\beta)^p = \Big(\sum_\sigma \sigma(\alpha\beta)\Big)^p = \sum_\sigma \sigma(\alpha\beta)^p + p\gamma$$

where γ is an integer by the multinomial expansion so

$$(T_{\mathbb{Q}}^K \alpha\beta)^p = T_{\mathbb{Q}}^K(\alpha\beta)^p + p\gamma$$

and since $p \mid T_{\mathbb{Q}}^K(\alpha\beta)^p$ we see that $p \mid (T_{\mathbb{Q}}^K \alpha\beta)^p$. Since p is a prime we see that $p \mid T_{\mathbb{Q}}^K \alpha\beta$.

Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis for $\mathbb{A} \cap K$. Then for $i = 1, \ldots, n$ we have $T_{\mathbb{Q}}^K(\alpha\omega_i)$ is divisible by p. We have

$$\alpha = a_1\omega_1 + \cdots + a_n\omega_n$$

with $a_1, \ldots, a_n$ integers. Since $\alpha \notin (p)$ hence $\alpha/p \notin \mathbb{A} \cap K$ we see that at least one of $a_1, \ldots, a_n$ is not divisible by p without loss of generality suppose $p \nmid a_1$.

Observe that since $p \mid T_{\mathbb{Q}}^K(\alpha\omega_i)$ we see that p divides

$$T_{\mathbb{Q}}^K(\alpha_1\omega_1 + \cdots + \alpha_n\omega_n)\omega_i = a_1 T_{\mathbb{Q}}^K \omega_1\omega_i + a_2 T_{\mathbb{Q}}^K \omega_2\omega_i + \cdots + a_n T_{\mathbb{Q}}^K \omega_n\omega_i.$$

By Theorem 25 we have

$$\begin{aligned}
a_1 D &= \det\begin{pmatrix} a_1 T_{\mathbb{Q}}^K(\omega_1\omega_1) & \cdots & a_1 T_{\mathbb{Q}}^K(\omega_1\omega_n) \\ T_{\mathbb{Q}}^K(\omega_2\omega_1) & \cdots & \vdots \\ \vdots & & \vdots \\ T_{\mathbb{Q}}^K(\omega_n\omega_1) & \cdots & T_{\mathbb{Q}}^K(\omega_n\omega_n) \end{pmatrix} \\
&= \det\begin{pmatrix} a_1 T_{\mathbb{Q}}^K(\omega_1\omega_1) + a_2 T_{\mathbb{Q}}^K(\omega_2\omega_1) + \cdots + a_n T_{\mathbb{Q}}^K(\omega_n\omega_1) & \cdots & a_1 T_{\mathbb{Q}}^K(\omega_1\omega_n) + \cdots + a_n T_{\mathbb{Q}}^K(\omega_n\omega_n) \\ T_{\mathbb{Q}}^K(\omega_2\omega_1) & \cdots & \\ \vdots & & \\ T_{\mathbb{Q}}^K(\omega_n\omega_1) & \cdots & T_{\mathbb{Q}}^K(\omega_n\omega_n) \end{pmatrix}
\end{aligned}$$

Since p divides each integer in the top row of the matrix we see that $p \mid a_1 D$. But $p \nmid a_1$ hence $p \mid D$ as required.

Let $[K : \mathbb{Q}] < \infty$. We define the norm of an ideal I of $\mathbb{A} \cap K$, denoted by NI,

$$NI = |\mathbb{A} \cap K/I|.$$

Thus NI is the number of residue classes modulo I. NI is also denoted by $N_{\mathbb{Q}}^{K}(I)$.

Theorem 49: Let $[K:\mathbb{Q}]=n$. Let I be a non-zero ideal of $\mathbb{A}\cap K$ and let $\alpha_1, \ldots, \alpha_n$ be an integral basis for I. Then

$$NI = \left|\frac{\operatorname{disc}(\alpha_1,\ldots,\alpha_n)}{D}\right|^{1/2},$$

where D is the discriminant of K.

Proof: We first remark that all integral bases for I have the same discriminant. This follows just as for the discriminant of K.

Let $\omega_1, \ldots, \omega_n$ be an integral basis for K. Then we can find an integral basis $\alpha_1, \ldots, \alpha_n$ of I of the form

$$\begin{aligned}
\alpha_1 &= a_{11}\omega_1\\
\alpha_2 &= a_{21}\omega_1 + a_{22}\omega_2\\
&\vdots\\
\alpha_n &= a_{n1}\omega_1 + \cdots + a_{nn}\omega_n
\end{aligned}$$

with $a_{ii}\in\mathbb{Z}^+$, by Theorem 38. Since

$$\operatorname{disc}\{\alpha_1,\ldots,\alpha_n\} = \left(\begin{pmatrix} a_{11} & & 0\\ \vdots & \ddots & \\ a_{n1} & \cdots & a_{nn}\end{pmatrix}\right)^2 D$$

we see that it suffices to show that

$$NI = a_{11}\cdots a_{nn}.$$

Suppose that

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

with $0\le r_i < a_{ii}$ for $i=1,\ldots,n$ and with $0\le s_i<a_{ii}$ ....

$$\begin{aligned}
&\implies (r_1-s_1)\omega_1+\cdots+(r_n-s_n)\omega_n\in I\\
&\implies (s_1-r_1)\omega_1+\cdots+(s_n-r_n)\omega_n\in I
\end{aligned}$$

Recall from the proof of Theorem 38 that a_{nn} is chosen to be minimal and positive.

$$\implies a_{nn}\mid r_n-s_n \implies r_n=s_n \text{ since } 0\le |r_n-s_n|<a_{nn}$$

Similarly $r_{n-1}=s_{n-1}, \ldots, r_1=s_1$.

Thus $NI\ge a_{11}\cdots a_{nn}$.

PMATH 641 Lecture 24: March 15, 2013

Theorem 44 ...
$\{\alpha_1,\ldots,\alpha_n\}$ a basis for I

$$\begin{aligned}
\operatorname{disc}\{\alpha_1,\ldots,\alpha_n\} &= \left(\begin{pmatrix} a_{11} & & 0\\ \vdots & \ddots & \\ a_{n1} & \cdots & a_{nn}\end{pmatrix}\right)^2 D\\
&= (a_{11}\cdots a_{nn})^2 D
\end{aligned}$$

We showed that $NI\ge a_{11}\cdots a_{nn}$.

To conclude suppose $\gamma \in \mathbb{A} \cap K$. Then $\gamma = b_1\omega_1 + \cdots + b_n\omega_n$ with $b_i \in \mathbb{Z}$; here $\{\omega_1, \dots, \omega_n\}$ is an integral basis for $\mathbb{A} \cap K$. Note that, by the Division Algorithm, $b_n = q_n a_{nn} + r_n$ with $0 \le r_n < a_{nn}$ and then $\gamma - q_n\alpha_n = d_1\omega_1 + \cdots + d_{n-1}\omega_{n-1} + r_n\omega_n$.

Repeating this $n-1$ times we find that there exist integers $q_1, \dots, q_{n-1}$ so that

$$\gamma - q_n\alpha_n - q_{n-1}\alpha_{n-1} + \cdots + q_1\alpha_1 = r_1\omega_1 + \cdots + r_n\omega_n$$

with $0 \le r_i < a_{ii}$. Thus

$$NI \le a_{11} \cdots a_{nn} \implies NI = a_{11} \cdots a_{nn}.$$

Corollary 50: $[K : \mathbb{Q}] < \infty$. Let α be a non-zero element of $\mathbb{A} \cap K$. Then $N(\alpha) = |N_{\mathbb{Q}}^K(\alpha)|$.
Proof: Let $\{\omega_1, \dots, \omega_n\}$ be an integral basis for $\mathbb{A} \cap K$. Then the principal ideal (α) has $\{\alpha\omega_1, \dots, \alpha\omega_n\}$ as an integral basis.

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

$$\begin{aligned} \operatorname{disc}\{\alpha\omega_1, \dots, \alpha\omega_n\} &= (\det(\sigma_i(\alpha\omega_j)))^2 \\ D = \operatorname{disc}\{\omega_1, \dots, \omega_n\} &= (\det(\sigma_i(\omega_j)))^2 \end{aligned}$$

But we have

$$\begin{aligned} \operatorname{disc}\{\alpha\omega_1, \dots, \alpha\omega_n\} &= \left(\det \begin{pmatrix} \sigma_1(\alpha) & & 0 \\ & \ddots & \\ 0 & & \sigma_n(\alpha) \end{pmatrix} \right)^2 \cdot D \\ &= (N_{\mathbb{Q}}^K(\alpha))^2 \cdot D. \end{aligned}$$

By Theorem 49 $\implies (N(\alpha))^2 = (N_{\mathbb{Q}}^K(\alpha))^2$. Thus $N(\alpha) = |N_{\mathbb{Q}}^K(\alpha)|$ since $N(\alpha)$ is a non-negative integer.

Theorem 51: (Fermat's Theorem) Let $[K : \mathbb{Q}] < \infty$ and let P be a prime ideal of $\mathbb{A} \cap K$. Let α be an element of $\mathbb{A} \cap K$ with $P \nmid (\alpha)$ then

$$\alpha^{NP-1} \equiv 1 \bmod P.$$

Proof: Let $\beta_1, \dots, \beta_{NP}$ be a complete set of representatives for the cosets $\mathbb{A} \cap K/P$ (in $\mathbb{A} \cap K$ modulo P). We may suppose β_{NP} is congruent to 0 mod P. Then since $P \nmid (\alpha)$ we see that

$$\alpha\beta_1, \dots, \alpha\beta_{NP}$$

is again a complete set of representatives mod P with $\alpha\beta_{NP}$ congruent to 0 modulo P. Therefore

$$\begin{aligned} \alpha\beta_1 \cdots \alpha\beta_{NP-1} &\equiv \beta_1 \cdots \beta_{NP-1} \bmod P. \\ \implies \alpha^{NP-1} &\equiv 1 \bmod P \end{aligned}$$

as required.

Proposition 52: Let $[K : \mathbb{Q}] < \infty$. Let A be a non-zero ideal of $\mathbb{A} \cap K$. Then $NA \in A$.
Proof: Let $\beta_1, \dots, \beta_{NA}$ be a complete set of representatives modulo A. Then

$$1 + \beta_1, \dots, 1 + \beta_{NP}$$

is also a complete set of representatives modulo A.

$$\begin{aligned} \implies \beta_1 + \cdots + \beta_{NA} &\equiv (1 + \beta_1) + \cdots + (1 + \beta_{NA}) \bmod A \\ 0 &\equiv NA \bmod A \end{aligned}$$

Notice that for any positive integer t there are only finitely many ideals A of $\mathbb{A} \cap K$ with $NA = t$.

Still to show: The norm map on ideals is multiplicative, i.e., for A, B ideals in $\mathbb{A} \cap K$

$$NAB = NA \cdot NB.$$

If we have this and

$$NA = p \text{ with } p \text{ a prime}$$

then A is a prime ideal. Further if p is a prime in $\mathbb{Z}$ then

$$N(p) = |N_{\mathbb{Q}}^{K} p| = p^n \text{ where } n = [K : \mathbb{Q}].$$

Every prime ideal P of $\mathbb{A} \cap K$ divides (p) for exactly one prime.

$$\implies NP = p^f$$

for some integer f with $1 \leq f \leq n$.

PMATH 641 Lecture 25: March 18, 2013

Let $[K : \mathbb{Q}] < \infty$. Let A and B be ideals of $\mathbb{A} \cap K$. We say that an ideal C of $\mathbb{A} \cap K$ is a greatest common divisor of A and B if it is a common divisor of A and B and all other common divisors of A and B divide it.

In fact there can be at most 1 greatest common divisor of A and B since if C and D are greatest common divisors of A and B then $C \mid D$ and $D \mid C$ hence $C \supseteq D$ and $D \supseteq C$ so $D = C$.

In fact there is one since if $A = (\alpha_1, \ldots, \alpha_n)$ and $B = (\beta_1, \ldots, \beta_s)$ then we may take $C = (\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$. Certainly $A \subseteq C$ and $B \subseteq C$ hence $C \mid A$ and $C \mid B$. Further if $D \mid A$ and $D \mid B$ then $D \supseteq A$ and $D \supseteq B$ hence $\alpha_1, \ldots, \alpha_r$ and $\beta_1, \ldots, \beta_s$ are in D so $D \supseteq C = (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$. Thus $D \mid C$. Therefore there is a unique greatest common divisor of A and B and we denote it by $\gcd(A, B)$.

$\gcd(A, B) = (1)$ is equivalent to A and B being coprime.

Since we have unique factorization into prime ideals in $\mathbb{A} \cap K$ if

$$A = p_1^{a_1} \cdots p_r^{a_r}$$

and

$$B = p_1^{b_1} \cdots p_r^{b_r}$$

with $p_1, \ldots, p_r$ distinct prime ideals and $a_1, \ldots, a_r, b_1, \ldots, b_r$ non-negative integers then

$$\gcd(A, B) = p_1^{c_1} \cdots p_r^{c_r}$$

where

$$c_i = \min(a_i, b_i) \text{ for } i = 1, \ldots, r.$$

Lemma 53: Let $[K : \mathbb{Q}] < \infty$. Let A and B be non-zero ideals of $\mathbb{A} \cap K$. Then there exists an element $\alpha \in A$ for which $\gcd(\frac{(\alpha)}{A}, B) = (1)$.
Proof: If $B = (1)$ the result is immediate. Suppose then that there are exactly r distinct prime ideals p_1, $\ldots$, p_r which divide B. We'll prove the result by induction on r.

First suppose that $r = 1$.
Choose α so that α is in A but not in Ap_1. This is possible since $A \neq Ap_1$. But then $\gcd((\alpha)/A, p_1)$ is a divisor of p_1. Since p_1 is a prime ideal it is either p_1 or (1). If it is p_1 so $\gcd((\alpha)/A, p_1) = p_1$ then $\gcd((\alpha), Ap_1) = Ap_1$. Thus $Ap_1 \mid (\alpha)$ hence $(\alpha) \subseteq Ap_1$ and so $\alpha \in Ap_1$ which is a contradiction.

Now suppose $r > 1$. Let

$$A_m = A \frac{P_1 \cdots P_r}{P_m}, \text{ for } m = 1, \ldots, r.$$

Choose α_m in A_m, by the case $r=1$, so that

$$\gcd\Big(\frac{(\alpha_m)}{A_m}, P_m\Big) = (1), \text{ for } m = 1, \ldots, r.$$

We now put

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

Since $\alpha_1 \in A_i$ and $A \mid A_i$ for $i = 1, \ldots, r$ we see that $\alpha_i \in A$ for $i = 1, \ldots, r$ we see that $\alpha_i \in A$ for $i = 1, \ldots, r$. Thus $\alpha \in A$.

Note that $\alpha \notin AP_m$ for $m = 1, \ldots, r$. To see this observe first that $AP_m \mid A_i$ whenever $i \neq m$. Therefore α_i is in AP_m for $i \neq m$. But $\alpha = \alpha_1 + \cdots + \alpha_r$ so if α is in AP_m for some m with $1 \leq m \leq r$ then α_m is in AP_m. But $\gcd((\alpha_m)/A_m, P_m) = (1)$.

Since $P_1, \ldots, P_r$ are distinct prime ideals

$$\gcd\Big(\frac{(\alpha_m)}{A}, P_m\Big) = (1). \tag{$*$}$$

$$\implies \gcd((\alpha_m), AP_m) = A.$$

But $\alpha_m \in AP_m$ so $(\alpha_m) \subseteq AP_m$ hence $AP_m \mid (\alpha_m)$. Thus $P_m \mid \frac{(\alpha_m)}{A}$ and this contradicts $*$.

We now show that $\gcd((\alpha)/A, B) = 1$. Suppose otherwise. Then $\gcd((\alpha)/A, B)$ is divisible by P_m for some integer m with $1 \leq m \leq r$. Then P_m divides $(\alpha)/A$ so AP_m divides (α). In particular $\alpha \in AP_m$ which is a contradiction.

PMATH 641 Lecture 26: March 20, 2013

Theorem 54: $[K : \mathbb{Q}] < \infty$. Let A and B be non-zero ideals of $\mathbb{A} \cap K$. Then

$$NAB = NA \cdot NB.$$

Proof: Let $\alpha_1, \ldots, \alpha_{NA}$ be a complete set of representatives modulo A. Similarly let $\beta_1, \ldots, \beta_{NB}$ be a complete set of representatives modulo B.

By Lemma 53 there exists γ in A for which $\gcd((\gamma)/A, B) = (1) \implies \gcd((\gamma), AB) = A$.

Consider the terms $\alpha_i + \gamma\beta_j$ with $1 \leq i \leq NA$ and $1 \leq j \leq NB$. These terms are all distinct mod AB since otherwise there exists i, j, k, l with $1 \leq i \leq NA$, $1 \leq j \leq NB$, $1 \leq k \leq NA$, $1 \leq l \leq NB$ for which

$$\alpha_i + \gamma\beta_j \equiv \alpha_k + \gamma\beta_l \pmod{AB}.$$

Then

$$\alpha_i - \alpha_k \equiv \gamma(\beta_j - \beta_l) \pmod{AB}.$$

Since γ is in A we see that $\alpha_i - \alpha_k \equiv 0 \pmod{A}$ hence $i = k$. But then

$$\gamma(\beta_j - \beta_l) \equiv 0 \pmod{AB}.$$

Thus $AB \mid (\gamma)(\beta_j - \beta_l)$

$$\begin{aligned} &\implies B \mid \frac{(\gamma)}{A}(\beta_j - \beta_l) \\ &\implies B \mid (\beta_j - \beta_l) \\ &\implies \beta_j \equiv \beta_l \pmod{B} \implies j = l \end{aligned}$$

Thus

$$NAB \geq NANB.$$

Suppose $\alpha \in \mathbb{A} \cap K$. Then $\alpha \equiv \alpha_i \pmod{A}$ for some i with $1 \le i \le NA$. Recall by $*$ $\gcd((\gamma), AB) = A$. Thus

$$\alpha - \alpha_i = \gamma \cdot \lambda + \delta$$

with $\lambda \in \mathbb{A} \cap K$ and $\delta \in AB$. Then $\lambda \equiv \beta_j \pmod{B}$ for some j with $1 \le j \le NB$. Therefore $\alpha = \alpha_i + \gamma\beta_j + \gamma(\lambda - \beta_j) + \delta$. Now since $\gamma \in A$ and $\lambda - \beta_j$ is in B we see that

$$\alpha \equiv \alpha_i + \gamma\beta_j \bmod AB.$$

Thus $NAB \le NA \cdot NB$ and so $NAB = NANB$.

Let $[K : \mathbb{Q}] < \infty$. We define a notation $\sim$ on the non-zero ideals of $\mathbb{A} \cap K$ by $A \sim B$ if and only if there exist α, $\beta \in \mathbb{A} \cap K$ with $\alpha\beta \ne 0$ so that

$$(\alpha)A = (\beta)B.$$

This is an equivalence relation

(1) $A \sim A \quad \alpha = \beta = 1$ ✓

(2) $A \sim B \iff B \sim A$ ✓

(3) If $A \sim B$ and $B \sim C$ then there exist α, β, γ, δ in $\mathbb{A} \cap K \setminus \{0\}$ such that $(\alpha)A = (\beta)B$ and $(\gamma)B = (\delta)C$ so then

$$(\alpha\gamma)A = (\alpha)(\gamma)A = (\gamma)(\beta)B = (\delta)(\beta)C = (\delta\beta)C.$$

Thus $A \sim C$.

The equivalence classes under the relation $\sim$ are known as the ideal classes of $\mathbb{A} \cap K$. Note that if we have just one equivalence class then all of the ideals are principal. The number of ideal classes is known as the class number of K and it is denoted by h or h_K.

Let $\mathcal{C} = \{\, [A] : A$ is an ideal of $\mathbb{A} \cap K \,\}$; here $[A]$ denotes the ideal class of which A is a representative.

We define a multiplication on $\mathcal{C}$ by

$$[A] \cdot [B] = [AB].$$

Note that this definition does not depend on the representatives chosen since if $A \sim C$ and $B \sim D$ then $AB \sim CD$.

Observe that $\mathcal{C}$ is an abelian group under multiplication. To see this note that multiplication is associative since

$$[A] \cdot ([B] \cdot [C]) = [A] \cdot [BC] = [A(BC)] = [(AB)C] = [AB] \cdot [C] = ([A] \cdot [B]) \cdot [C].$$

The principal ideal class is the identity element of the group since $[(1)] \cdot [B] = [B] = [B] \cdot [(1)]$. Plainly also $[A] \cdot [B] = [B] \cdot [A]$.

Further $[A]$ has an inverse. To see this note that there is a positive integer a in A (take $\alpha \in A \ldots$) since A is not (0).

Thus $(a) \subseteq A$ hence $A \mid (a)$. Therefore there exists an ideal B with $AB = (a)$. Thus $[A] \cdot [B] = [(a)] = [(1)]$ and so

$$[B] = [A]^{-1}.$$

Therefore $\mathcal{C}$ is an abelian group under $\cdot$.

PMATH 641 Lecture 27: March 22, 2013

h: class number of K
$[K : \mathbb{Q}] < \infty$. h is *finite* as we'll show.

Another important invariant of K is the regulator R. It often arises together with h.

Suppose that $[K:\mathbb{Q}] < n$ and there exist r_1 real embeddings of K in $\mathbb{C}$ and $2r_2$ embeddings which are not into $\mathbb{R}$. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings and let $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ be the other embeddings where we arrange that

$$\sigma_{r_1+i} = \overline{\sigma_{r_1+r_2+i}} \text{ for } i = 1, \ldots, r_2.$$

Thus $r_1 + 2r_2 = n$. Put

$$r = r_1 + r_2 - 1.$$

Let $U(K)$ be the group of units in $\mathbb{A} \cap K$. Dirichlet proved that

$$U(K) \approx \mathrm{Tor} \times \mathbb{Z}^r$$

where Tor is a finite group corresponding to the roots of unity in K.

In particular there exist a system of fundamental units $\epsilon_1, \ldots, \epsilon_r$ such that if ϵ is in $U(K)$ then there exists a root of unity ζ and integers $a_1, \ldots, a_r$ such that

$$\epsilon = \zeta \epsilon_1^{a_1} \cdots \epsilon_r^{a_r}.$$

Note that if (a_{ij}) is an $r \times r$ matrix with integer entries which has an inverse with integer entries then

$$\{\epsilon_1^{a_{11}} \cdots \epsilon_r^{a_{1r}}, \ldots, \epsilon_1^{a_{r1}}, \ldots, \epsilon_r^{a_{rr}}\}$$

is again a fundamental system of units.

Let $L\colon K^* \to \mathbb{R}^{r_1+r_2}$ be the logarithmic embedding of K^* in $\mathbb{R}^{r_1+r_2}$ given by

$$L(\alpha) = (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_{r_1}(\alpha)|, 2\log|\sigma_{r_1+1}(\alpha)|, \ldots, 2\log|\sigma_{r_1+r_2}(\alpha)|).$$

The kernel of L consists of the roots of unity of K. Further if $\alpha \in K$ with $\alpha \neq 0$ then

$$\begin{aligned} \log|N_{\mathbb{Q}}^K(\alpha)| &= \log|\sigma_1(\alpha)| + \cdots + \log|\sigma_{r_1+2r_2}(\alpha)| \\ &= \log|\sigma_1(\alpha)| + \cdots + \log|\sigma_{r_1}(\alpha)| + 2\log|\sigma_{r_1+1}(\alpha)| + \cdots + 2\log|\sigma_{r_1+r_2}(\alpha)| \end{aligned}$$

Notice that if $\alpha \in U(K)$ then $L(\alpha)$ lies in the subgroup of $\mathbb{R}^{r_1+r_2}$ given by $x_1 + \cdots + x_{r_1+r_2} = 0$. In fact they determine a lattice of rank $r_1 + r_2 - 1$. We can ask for the volume of a fundamental region of the lattice. This is called the regulator R. Equivalently

$$R = \left| \det(e_i \log|\sigma_i(\epsilon_j)|)_{\substack{i=1,\ldots,r \\ j=1,\ldots,r}} \right|$$

where $e_i = 1$ if $1 \leq i \leq r_1$ and $e_i = 2$ otherwise.

For $[K:\mathbb{Q}] = 2$ with K real quadratic then $R = \log \epsilon$ where ϵ is the fundamental unit larger than 1. If K is imaginary quadratic take

$$R = 1.$$

Let $M_K(x)$ be the number of ideals of $\mathbb{A} \cap K$ with norm at most x. One can prove

$$\lim_{x \to \infty} \frac{M_K(x)}{x} = 2^{r_1} (2\pi)^{r_2} \frac{hR}{W\sqrt{|d|}}$$

where W is the number of roots of unity in K. The number of integers up to x is $x + O(1)$. The number of primes $\pi(x)$ up to x satisfies

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Let $\pi_K(x)$ denote the number of prime ideals up to x. Landau proved that

$$\lim_{x\to\infty} \frac{\pi_K(x)}{x/\log x} = 1.$$

$$\begin{aligned}\zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \\ &= \prod_p \Big(\frac{1}{1-\frac{1}{p^s}}\Big)\end{aligned}$$

PMATH 641 Lecture 28: March 25, 2013

Corrections to Question 4 on the assignment. Replace "Let d be the discriminant of K..." by "Let d be the discriminant of θ...". Also "...of the form

$$\frac{1}{d}(a_0 + a_1\theta + \cdots + a_{i-1}\theta^{i-1})$$

with a_0, a_1, ..., a_{i-1} integers and a_{i-1}..."

Theorem 55: Let $[K:\mathbb{Q}] < \infty$. There exists a positive number C_0 which depends on K such that if A is a non-zero ideal of $\mathbb{A}\cap K$ then there exists a non-zero element α of A for which

$$|N_{\mathbb{Q}}^K(\alpha)| \leq C_0 NA.$$

Proof: Let ω_1, ..., ω_n be an integral basis for K. Next put

$$t = [(NA)^{1/n}]$$

and consider the elements β in $\mathbb{A}\cap K$ of the form

$$a_1\omega_1 + \cdots + a_n\omega_n \tag{$*$}$$

with $0 \leq a_i \leq t$ for $i = 1, \ldots, n$. There are $(t+1)^n$ such elements and since $(t+1)^n > NA$ there exist β_1, β_2 of the form $*$ which are equivalent modulo A. In particular $\alpha = \beta_1 - \beta_2 = b_1\omega_1 + \cdots + b_n\omega_n$ where $0 \leq |b_i| \leq t$.

Then let σ_1, ..., σ_n be the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$. Thus

$$\begin{aligned}|N_{\mathbb{Q}}^K(\alpha)| &= \prod_{i=1}^{n} |\sigma_i(b_1\omega_1 + \cdots + b_n\omega_n)| \\ &\leq t^n \Big(\prod_{i=1}^{n} n\big(\max_{1\leq j\leq n} |\sigma_i(\omega_j)|\big)\Big) \\ &\leq NA\cdot C_0{}^{4)}\end{aligned}$$

Theorem 56: Let $[K:\mathbb{Q}] < \infty$. The class number of K is finite.
Proof: We'll show that every non-zero ideal of $\mathbb{A}\cap K$ is equivalent to an ideal of norm at most C_0, where C_0 is from Theorem 55. Since there are only finitely many ideals of norm at most C_0 the result then follows.

Let I be a non-zero ideal of $\mathbb{A}\cap K$. Then there exists an ideal A such that $AI \sim (1)$.

By Theorem 55 there exists a non-zero α in A for which

$$|N_{\mathbb{Q}}^K(\alpha)| \leq C_0 NA.$$

4) where C_0 is above quantity

Note that $\alpha \in A \implies (\alpha) \subseteq A$ so $A \mid (\alpha)$ hence there exists B such that $AB = (\alpha)$. But

$$NA \cdot NB = NAB = N(\alpha) = |N_{\mathbb{Q}}^{K}(\alpha)| \leq C_0 NA.$$

Thus $NB \leq C_0$.

Further $AB \sim (1)$ and since $AI \sim (1) \implies B \sim I$. Thus I is equivalent to an ideal of norm at most C_0.

If h is the class number of K then by Lagrange's Theorem for any non-zero ideal A of $\mathbb{A} \cap K$ we have

$$[A]^h = [(1)].$$

Equivalently A^h is principal for any ideal A.

Suppose q is a positive integer coprime with h and $A^q \sim B^q$ then $A \sim B$. To see this note that if $\gcd(q, h) = 1$ then there exists r, s with $rq + sh = 1$ and then

$$A^{rq} \sim B^{rq} \text{ so } A^{1-sh} \sim B^{1-sh} \implies A \sim B.$$

It can be shown that we can take $C_0 = \sqrt{|d|}$ where d is the discriminant of K.

Example: Consider $K = \mathbb{Q}(\sqrt{-5})$. We have $d = -20$ so $C_0 = \sqrt{20}$. Therefore we need only consider ideals of norm at most $\sqrt{20}$ hence at most 4 we must check how (2) and (3) decompose into prime ideals in $\mathbb{A} \cap \mathbb{Q}(\sqrt{-5})$.

$$\begin{aligned}
(2) &= (2, 1+\sqrt{-5})(2, 1-\sqrt{-5}) \\
&= (4, 2-2\sqrt{-5}, 2+2\sqrt{-5}, 6) \\
&= (2, 2(1+\sqrt{-5})) \\
&= (2)
\end{aligned}$$

PMATH 641 Lecture 29: March 27, 2013

Class number of $\mathbb{Q}(\sqrt{-5})$. It suffices to consider ideals of norm at most 4. Note that

$$(2, 1+\sqrt{-5}) \cdot (2, 1-\sqrt{-5}) = (4, 2(1+\sqrt{-5}), 2(1-\sqrt{-5}), 6) = (2).$$

Also observe that

$$2 - (1+\sqrt{-5}) = 1 - \sqrt{-5}$$

and so

$$(2, 1+\sqrt{-5}) = (2, 1-\sqrt{-5}).$$

Put $\mathcal{P} = (2, 1+\sqrt{-5})$. Thus $(2) = \mathcal{P}^2$. Also note that

$$(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (9, 3(1+\sqrt{5}), 3(1-\sqrt{5}), 6) = (3).$$

Put $\mathcal{Q} = (3, 1+\sqrt{-5})$ and $\mathcal{Q}' = (3, 1-\sqrt{-5})$. We have $N\mathcal{Q}N\mathcal{Q}' = 9$.

Could we have $N\mathcal{Q} = 1$? Then $\mathcal{Q} = (1)$. In particular $1 \in \mathcal{Q}$ hence there exist a, b, c, $d \in \mathbb{Z}$ with

$$3(a + b\sqrt{-5}) + (1+\sqrt{-5})(c + d\sqrt{-5}) = 1.$$

$$\begin{aligned}
\implies 3a + c - 5d &= 1 \\
3b + c + d &= 0 \\
\hline
3a - 3b - 6d &= 1
\end{aligned}$$

and since $3 \nmid 1$. #

Similarly $N\mathcal{Q}' \neq 1$ hence $N\mathcal{Q} = N\mathcal{Q}' = 3$ and $\mathcal{Q}$ and $\mathcal{Q}'$ are prime ideals. Thus (1), $\mathcal{P}$, $\mathcal{P}^2$, $\mathcal{Q}$, and $\mathcal{Q}'$ are the ideals of norm at most 4. Since $\mathcal{P}^2$ is principal

$$\mathcal{P}^2 \sim (1)$$

and so we need to consider only the ideal classes of (1), $\mathcal{P}$, $\mathcal{Q}$, and $\mathcal{Q}'$.

We have

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

$$\mathcal{Q}\mathcal{P} \sim (1).$$

$$(3, 1-\sqrt{-5})(2, 1+\sqrt{-5}) = (1-\sqrt{-5})$$

$$\left.\begin{aligned} \mathcal{Q}'\mathcal{P} &\sim (1) \\ \mathcal{Q}\mathcal{P} &\sim (1) \end{aligned}\right\} \implies \mathcal{Q} \sim \mathcal{Q}'$$

$$\left.\begin{aligned} \mathcal{Q}\mathcal{Q}' &\sim (1) \\ \mathcal{Q}\mathcal{P} &\sim (1) \end{aligned}\right\} \implies \mathcal{Q}' \sim \mathcal{P}$$

Thus

$$\mathcal{C} = \{[(1)], [\mathcal{P}]\}.$$

Could we have $\mathcal{P} \sim (1)$, so $\mathcal{P}$ principal? Then $\mathcal{P} = (a + b\sqrt{-5})$ and since $N\mathcal{P} = 2$

$$a^2 - 5b^2 = 2 \implies a^2 \equiv 2 \pmod 5 \qquad \#.$$

Therefore $h = 2$.

Suppose $[K : \mathbb{Q}] < \infty$.

There is an extension E of K which is Galois over K and has the property that the Galois group of E over K is isomorphic to the ideal class group of K. Also every ideal of $\mathbb{A} \cap K$ becomes principal in E.

E is the Hilbert class field of K.

PMATH 641 Lecture 30: April 1, 2013

Lattices, $\mathit{\Lambda}$ in $\mathbb{R}^n$

Let $\alpha_1, \ldots, \alpha_n$ be linearly independent vectors over $\mathbb{R}$ in $\mathbb{R}^n$. The set of points

$$\mathit{\Lambda} = \{\, m_1\alpha_1 + \cdots + m_n\alpha_n : m_i \in \mathbb{Z},\, i = 1, \ldots, n \,\},$$

is known as a lattice. The lattice is said to be generated by $\alpha_1, \ldots, \alpha_n$. Notice that if (v_{ij}) is a matrix with integer entries and $\det(v_{ij}) = \pm 1$ and we put

$$\alpha_i' = \sum_{j=1}^{n} v_{ij}\alpha_j$$

then $\alpha_1', \ldots, \alpha_n'$ is also a basis for $\mathit{\Lambda}$.

Put $d(\mathit{\Lambda}) = |\det(\alpha_1, \ldots, \alpha_n)|$. Then $d(\mathit{\Lambda})$ does not depend on the choice of generators $\alpha_1, \ldots, \alpha_n$ for $\mathit{\Lambda}$ since

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

whenever $\alpha_1', \ldots, \alpha_n'$ also generate $\mathit{\Lambda}$.

For generators $\alpha_1, \ldots, \alpha_n$ of Λ we can define an associated fundamental parallelogram P in $\mathbb{R}^n$ given by

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

Notice that every element β in $\mathbb{R}^n$ has a unique representation in the form

$$\beta = \lambda + \gamma,$$

with $\lambda \in \Lambda$ and $\gamma \in P$.

Note also that $\mu(P)$ the Lebesgue measure or volume of P is just

$$\mu(P) = d(\Lambda).$$

Remark: Since $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{R}$, $d(\Lambda) > 0$.
Example: Let Λ be the lattice in $\mathbb{R}^n$ generated by $e_1, \ldots, e_n$ where

$$e_j = (0, \ldots, 0, \overset{j\text{th position}}{1}, 0, \ldots, 0)$$

$$\Lambda_0 = \{\, (m_1, \ldots, m_n) : m_i \in \mathbb{Z} \text{ for } i = 1, \ldots, n \,\}.$$

$d(\Lambda_0) = 1$

Theorem 57: (Blichfeldt's Theorem) Let $m, n \in \mathbb{Z}^+$. Let Λ be a lattice in $\mathbb{R}^n$. Let S be a set in $\mathbb{R}^n$ with Lebesgue measure $\mu(S)$. Suppose that either $\mu(S) > md(\Lambda)$ or S is compact and

$$\mu(S) \geq md(\Lambda)$$

then there exist distinct points $x_1, \ldots, x_{m+1}$ in S with with $x_i - x_j \in \Lambda$ for $1 \leq i, j \leq m$.
Proof: Let $\alpha_1, \ldots, \alpha_n$ generate Λ and let P be the fundamental parallelogram associated with $\alpha_1, \ldots, \alpha_n$.

For each $\lambda \in \Lambda$ we define $R(\lambda)$ to be the set of points $v \in P$ such that

$$\lambda + v \in S.$$

We then have

$$\sum_{\lambda \in \Lambda} \mu(R(\lambda)) = \mu(S) > md(\Lambda) = m\mu(P).$$

Therefore there is a point $v_0 \in S$ which is associated with $m + 1$ distinct lattice points $\lambda_1, \ldots, \lambda_{m+1}$. We now take $x_i = v_0 + \lambda_i$ for $i = 1, \ldots, m + 1$. But then

$$x_i - x_j = \lambda_i - \lambda_j \in \Lambda$$

as required.

Suppose now that S is compact and

$$\mu(S) = md(\Lambda).$$

Let $\epsilon_1, \epsilon_2, \ldots$ be a sequence of *positive* real numbers with $\lim_{r\to\infty} \epsilon_r = 0$. Then

$$\mu((1 + \epsilon_r)S) > \mu(S) = md(\Lambda).$$

Thus there exist points $x_{1,r}, \ldots, x_{m+1,r}$ in $(1 + \epsilon_r)S$ for which

$$u_r(i, j) = x_{i,r} - x_{j,r} \in \Lambda \qquad \text{for } 1 \leq i, j \leq m + 1.$$

Since S is compact we can extract a subsequence and so suppose that $\lim_{r\to\infty} x_{i,r} = x_i'$ for $i = 1, \ldots, m + 1$ with $x_i' \in S$. Notice that since Λ is discrete the $u_r(i, j)$'s are all the same for r sufficiently large. Therefore $x_1', \ldots, x_{m+1}'$ are in S and

$$x_i' - x_j' \in \Lambda \qquad \text{for } 1 \leq i, j \leq m + 1.$$

PMATH 641 Lecture 31: April 3, 2013

? from last class: Note that

$$\frac{1}{1+\epsilon_r} x_{i,r} \in S.$$

Definition: Let S be a subset of $\mathbb{R}^n$. We say that S is symmetric about the origin if whenever $x \in S$ then $-x \in S$. We say that S is convex if whenever x, y are in S then $\lambda x + (1-\lambda)y \in S$ for any $\lambda \in \mathbb{R}$ with $0 \leq \lambda < 1$.

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

$$\mu(S) > m2^n d(\mathit{\Lambda})$$

or

$$\mu(S) \geq m2^n d(\mathit{\Lambda})$$

and S is compact then there exist m pairs of non-zero points $\pm\lambda_1, \pm\lambda_2, \ldots, \pm\lambda_m$ from $\mathit{\Lambda}$ and in S.
Proof: We apply Theorem 57 to $\frac{1}{2}S$. Note that $\mu(\frac{1}{2}S) = \frac{1}{2^n}\mu(S)$. Therefore there exist distinct non-zero points $\frac{1}{2}x_1, \ldots, \frac{1}{2}x_m$ in $\frac{1}{2}S$ which have the property that

$$\frac{1}{2}x_i - \frac{1}{2}x_j \in \mathit{\Lambda} \qquad \text{for } 1 \leq i, j \leq m.$$

Let us suppose without loss of generality that

$$x_1 \stackrel{\sim}{>} x_2 \stackrel{\sim}{>} \cdots \stackrel{\sim}{>} x_m$$

where $\stackrel{\sim}{>}$ indicates that the first non-zero coordinate in $x_i - x_{i+1}$ is positive for $i = 1, \ldots, m-1$. We now take

$$\lambda_j = \frac{1}{2}x_j - \frac{1}{2}x_{m+1} \qquad \text{for } j = 1, \ldots, m.$$

Note that since S is symmetric about $\mathbf{0}$ we see that $-x_{m+1}$ is in S. Since S is convex

$$\frac{1}{2}x_j + \frac{1}{2}(-x_{m+1}) = \frac{1}{2}x_i - \frac{1}{2}x_{m+1} = \lambda_j$$

is in S.

$\implies \lambda_1, \ldots, \lambda_m$ are non-zero and distinct with first non-zero coordinate positive. Also $-\lambda_1, \ldots, -\lambda_m$ are in S, by symmetry, and in $\mathit{\Lambda}$. The result follows.

Observe that the lower bounds in the theorem can't be improved. Take

$$S = \{ (x_1, \ldots, x_n) \in \mathbb{R}^n : |x_1| < m \text{ and } |x_2| < 1, \ldots, |x_n| < 1 \}.$$

$\mu(S) = m2^n$. S is convex and symmetric about $\mathbf{0}$. Take the lattice $\mathit{\Lambda}_0$ with $d(\mathit{\Lambda}_0) = 1$. The points of $\mathit{\Lambda}_0$ is in S are $(\pm j, 0, \ldots, 0)$ for $j = 0, \ldots, m-1$.

Suppose $[K : \mathbb{Q}] = n$ and let $K = \mathbb{Q}(\theta)$. Suppose $\theta = \theta_1, \ldots, \theta_n$ are the conjugates of θ over $\mathbb{Q}$. Suppose that $\sigma_1, \ldots, \sigma_n$ are the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$. Let r_1 be the number of embeddings in $\mathbb{R}$, equivalently the number of $\theta_1, \ldots, \theta_n$ which are in $\mathbb{R}$. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ be the other embeddings, with $\sigma_{r_1+j} = \overline{\sigma_{r_1+r_2+j}}$ for $j = 1, \ldots, r_2$.

Let $\tilde{\sigma} \colon K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be given by

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

$\tilde{\sigma}$ is an injective ring homomorphism. We may identify $\mathbb{C}$ with $\mathbb{R}^2$ by considering real and imaginary parts. Let us define

$$\sigma\colon K \to \mathbb{R}^n$$

by

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

Lemma 59: $[K : \mathbb{Q}] < \infty$. A a non-zero ideal in $\mathbb{A} \cap K$. Then $\sigma(A)$ is a lattice in $\mathbb{R}^n$ with

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

where D is the discriminant of K.

PMATH 641 Lecture 32: April 5, 2013

Recall our map $\sigma\colon K \to \mathbb{R}^n$ given by

$$\sigma(x) = \big(\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re(\sigma_{r_1+1}(x)), \Im(\sigma_{r_1+1}(x)), \ldots, \Re(\sigma_{r_1+r_2}(x)), \Im(\sigma_{r_1+r_2}(x))\big).$$

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

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

where D is the discriminant of K.

Proof: Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for A. The coordinates of $\sigma(\alpha_i)$ in $\mathbb{R}^n$ are

$$\big(\sigma_1(\alpha_i), \ldots, \sigma_{r_1}(\alpha_i), \ldots, \Im(\sigma_{r_1+r_2}(\alpha_i))\big). \qquad (*)$$

Note that for $z \in \mathbb{C}$, $\Re(z) = \frac{z+\overline{z}}{2}$ and $\Im(z) = -\frac{z-\overline{z}}{2} = -\frac{1}{i}\big(\overline{z} - \big(\frac{z+\overline{z}}{2}\big)\big)$. Thus

$$D = \det(\sigma_i(\alpha_j)) = \Big(\frac{1}{-2i}\Big)^{r_2} d(\Lambda)$$

where $d(\Lambda)$ is the determinant of the matrix whose ith row is $*$. Since $D \neq 0$ we see that $d(\Lambda)$ is not 0 and so $\sigma(A) = \Lambda$ is a lattice in $\mathbb{R}^n$. Now by Theorem 49 our result follows.

Theorem 60: Suppose $[K : \mathbb{Q}] = n$ with $n = r_1 + 2r_2$ where r_1 is the number of real embeddings of K in $\mathbb{C}$ and $2r_2$ is the number of other embeddings. Let A be a non-zero ideal in $\mathbb{A} \cap K$. Then there exists a non-zero α in A for which

$$|N_{\mathbb{Q}}^K(\alpha)| \leq \Big(\frac{2}{\pi}\Big)^{r_2} \sqrt{|D|} NA.$$

Proof: Let $t \in \mathbb{R}^+$ and let S_t be the set of $(x_1, \ldots, x_n)$ in $\mathbb{R}^n$ for which $|x_i| \leq t$ for $i = 1, \ldots, r_1$ and for which $x_{r_1+j}^2 + x_{r_1+1+j}^2 \leq t^2$ for $j = 1, 3, 5, \ldots, 2r_2 - 1$.

Note that S_t is compact, convex and symmetric about the origin $\mathbf{0}$. Further

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

We now take

$$t = \Big(\frac{2^n}{2^{r_1+r_2}\pi^{r_2}}|D|^{1/2}NA\Big)^{1/n}.$$

Then

$$\mu(S_t) = 2^n\Big(\frac{|D|^{1/2}NA}{2^{r_2}}\Big) = 2^n d(\Lambda),$$

where Λ is the lattice associated with the ideal A. By Minkowski's Theorem there is a non-zero lattice point of Λ in S_t. Let α be the associated element of A. Then, let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$,

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

Suppose $[K:\mathbb{Q}]=n$. Let θ be in $\mathbb{A}\cap K$ and such that $K=\mathbb{Q}(\theta)$. Let f be the minimal polynomial of θ. Let t be the index of $\mathbb{Z}[\theta]$ in $\mathbb{A}\cap K$. Let p be a prime in $\mathbb{Z}$.

? How does (p) decompose in $\mathbb{A}\cap K$? Consider f in $\mathbb{F}_p[x]$ where $\mathbb{F}_p$ is the finite field of p elements. Identify $\mathbb{F}_p$ with $\mathbb{Z}/p\mathbb{Z}$. Suppose $p\nmid t$. In $\mathbb{F}_p[x]$,

$$f(x) = f_1(x)^{e_1}\cdots f_g(x)^{e_g}$$

where f_i is irreducible in $\mathbb{F}_p[x]$ of degree d_i. We have

$$(p) = P_1^{e_1}\cdots P_g^{e_g}$$

where P_i is a prime ideal in $\mathbb{A}\cap K$. In fact

$$P_i = (p, f_i(\theta)).$$

If also $p\nmid D$ then $e_1=\cdots=e_g=1$. Thus

$$n = d_1+\cdots+d_g \tag{$*$}$$

and so is a partition of n.

Let $\theta=\theta_1, \ldots, \theta_n$ be the conjugates of θ over $\mathbb{Q}$ and put $L=\mathbb{Q}(\theta_1,\ldots,\theta_n)$. Let $G=\mathrm{Gal}(L/\mathbb{Q})$ be the Galois group of L over $\mathbb{Q}$. If σ is in $\mathrm{Gal}(L/\mathbb{Q})$ then σ induces a permutation of $\theta_1, \ldots, \theta_n$ and so an element $\tilde{\sigma}$ of S_n. We can decompose $\tilde{\sigma}$ as a product of cycles say $\tilde{\sigma}=c_1\cdots c_l$ and then

$$n = |c_1|+\cdots+|c_l| \tag{$**$}$$

where $|c_i|$ is the length of the cycle c_i. $**$ is another partition of n.

1880 Frobenius

$$\frac{\#\text{ of primes up to } x \text{ with a given partition } *}{\#\text{ of primes up to } x} \to \text{tends to a limit.}$$

and the limit is the proportion of elements σ of G with the same partition of n in $**$.

Office Hours
Mon Apr 8 2:40–3:40
Wed Apr 10 2:00–3:00
Thurs Apr 11 2:00–3:00