Notes for Cryptography

Professor Brian Sittinger

2/15/16

1 Introduction

Last HW had 4 units, this HW will have 6.

2 Lecture Start

Let K be an algebraic number field over $\mathbb{Q}$. Its ring of algebraic integers is denoted $\mathcal{O}$ or $(\mathcal{O}_k)$. Note that $\mathcal{O} = K \cap \mathbb{B}$ Where $\mathbb{B}$ is the set of all algebraic integers.

A field extension is said to be algebraic if all integers in the field extension are algebraic over $\mathbb{Q}$. This is a hint for #7.

We now turn to the conecept of an Integral basis. Let $[K : Q] = n$. We know that $K = Q(\theta)$ for some alebraic number or integer θ. This implies that

$$\{1, \theta, \ldots, \theta^{n-1}\}$$

is a basis for K over Q. IS ther some kind of analogous basis for $\mathcal{O}$? Yes, there is. An "integral basis." A $\mathbb{Z}$ basis

$$\{\alpha_1, \alpha_2, \ldots, \alpha_s\}$$

for $\mathcal{O}$ is called an integral basis for K or for O. Any x in $\mathcal{O}$ can be unidquely written as

$$x = \sum_{j=1}^{s} c_j \alpha_j$$

Note that any integral basis for K or $\mathcal{O}$ is automatically a Q-basis for K in particular $s = \frac{n}{[K:\mathbb{Q}]}$. An integral basis exists. Integer basis are not always "obvious." For example, if $K = Q(\sqrt{5})$. What would be an obvious example of an an integral basis. It might seem to be $\{1, \sqrt{5}\}$, but this is not the case. Thus K does not have an integral basis, and

$$\mathcal{O} \supset \mathbb{Z}[\sqrt{5}]$$

For instance $\frac{1+\sqrt{5}}{2}$ is an algebraic integer in K since it's a root of $x^2 - x + 1 = 0$. How do we compute integral bases? There is a useful algorithm for this. This hinges on discriminant calculations. Recall that if

$$\{\alpha_1, \ldots, \alpha_n\}$$

be a basis for K over $\mathbb{Q}$

$$\Delta[\alpha_1, \ldots, \alpha_n] \equiv \{\det(\sigma_i(\alpha_j))\}^2$$

If we pick another basis $\{\beta_1, \ldots, \beta_n\}$ for K over Q. Then there exists an invertible change of basis matrix $c_{ij} \in \mathbb{Q}$ such that $\beta_j = \sum_{i=1}^{n} c_{ij}\alpha_i, j = 1, \ldots, n$. What this gives us is that

$$\Delta[\beta_1, \ldots, \beta_n] = (\det\ C)^2 \cdot \Delta[\alpha_1, \ldots, \alpha_n]$$

since determinants are multiplicative. Suppose $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{O}$ is a basis for K over $\mathbb{Q}$. Then if $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, then $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis for $\mathcal{O}$. Finally, let $\{\beta_1, \ldots, \beta_n\}$ be an integral basis for $\mathcal{O}$. As in the previous discussion, $\alpha = \sum_{j=1}^{n} c_{ij}\beta_j, c_{ij} \in \mathbb{Z}$. Then as before,

$$\Delta[a_1, \ldots, a_n] = (\det\ c_{ij})^2 \Delta[\beta_1, \ldots, \beta_n]$$

We said that $\Delta[a_1, \ldots, a_n]$ is square-free but, we have an apparent square of an integer determinant. Thus $\det\ c_{ij} = \pm 1$. Then

$$A^{-1} = \frac{1}{|\Delta|}(A_{adj})$$

Therefore if $\{\beta_1, \ldots, \beta_n\}$ is an integer then $\{\alpha_1, \ldots, \alpha_n\}$ is an integer basis. From this we can see that if we have a square free descriminant, we are home free as far as fininding an integer basis. The converse is not always true, that given an integral basis the discriminant is not always square-free. The discriminent of a number field K is the discriminant of its integral basis (being well defined). Also the discriminant of a number field is always an integer. Proposition 2.21: Suppose we let $[K : Q] = n$ with $\mathbb{Z}$ basis $\{\alpha_1, \ldots, \alpha_n\}$ Let G be an additive subgroup of $\mathcal{O}$ If $G \neq \mathcal{O}$ then there exists an algebraic integer of the form

$$(\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n)/p$$

where each $\lambda_i \in \{0, \ldots, p-1\}$ and $p^2 | \Delta G$.

3 Computing an integral basis

1. start with an initial guess G for $\mathcal{O}$ with $n = [k : Q]$ basis alts of algebraic integers.

2. Compute the discriminent Δ_G.

3. for each prime p such that $p^2|\Delta_G$, test all elts of the form $(\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n)/p$ to see if any of these are algebraic integers. Use Norms and Traces to rule out obvious non-candidtates. Else check minimum polynomials.

4. If new algebraic integers arise, enlarge G to G' repeat steps 2—3 as necessary.

4 Examples of integral bases

Consider $K = Q(\sqrt{d})$, d is square free. Guess for an integral basis: $\{1, \sqrt{d}\}$. Then

$$\Delta_G = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix} = 4d$$

The there exists poss alegebraic integer of the form

$$\alpha = \frac{1}{2}(\lambda_1 + \lambda_2\sqrt{d}), \lambda_1, \lambda_2 \in \{0, 1\}$$

Then

$$\mathrm{Tr}(\alpha) = \frac{1}{2}(\lambda_1 + \lambda_2\sqrt{d}) + \frac{1}{2}(\lambda_1 - \lambda_2\sqrt{d}) = \lambda_1 \in \mathbb{Z}$$

$$N(\alpha) = \frac{1}{2}(\lambda_1 + \lambda_2\sqrt{d})\frac{1}{2}(\lambda_1 - \lambda_2\sqrt{d}) = \frac{1}{4}(\lambda_1^2 - d\lambda_2^2)$$

This means that

$$(\lambda_1, \lambda_2) \neq (1, 0), (0, 1)$$

What about $\lambda_1 = \lambda_2 = 1$ so $\alpha = \frac{1+\sqrt{d}}{2}$ Then $d = 1 \pmod 4$. If $d \neq 1 \pmod 4$. then there does not exist algorithmic integers of the form $(\lambda_1 + \lambda_2\sqrt{d})/2$. What if $d = 1 \mod 4$? Then

$$\alpha = \frac{1 + \sqrt{d}}{2}$$

$$\alpha^2 - \alpha + \frac{1 - \lambda}{4} = 0$$

monic with $\mathbb{Z}$ coeficients.

Fun fact — if we let $K = Q(\sqrt{d})$, d squarefree and $d \not\equiv 1 \mod 4$. Then $\mathcal{O}$ has integral basis $\{1, \sqrt{d}\}$ discrimanent $4d$. If $d = 1 \mod 4$ then $\mathcal{O}$ has integral basis $\{1, \frac{1+\sqrt{d}}{2}\}$ discrimanent d.

Example 2, let $K = Q(5^{1/3})$. Our first guess for a basis is

$$\{1, 5^{1/3}, 5^{2/3}\}$$

Embeddings:

$$\sigma_1 : 1 \to 1, \theta \to \theta, \theta^2 \to \theta^2$$

$$\sigma_2 : 1 \to 1, \theta \to \omega\theta, \theta^2 \to \omega^2\theta^2$$

$$\sigma_3 : 1 \to 1, \theta \to \omega^2\theta, \theta^2 \to \omega^4\theta^2 = \omega\theta^2$$

Where $\theta = 5^{1/3}$ and ω is a 3rd root of unity. So

$$\Delta_G = \begin{vmatrix} 1 & \theta & \theta^2 \\ 1 & \omega\theta & \omega^2\theta^2 \\ 1 & \omega^2\theta & \omega\theta^2 \end{vmatrix} = -3^3 5^2$$

As said in the textbook (Prop 2.18) we let $k = Q(\theta)$, deg n,

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{\frac{n(n-1)}{2}} N(p'(\theta))$$

Where p' is the derivative.

$$\Delta_G = (-1)^{\frac{3\cdot 2}{2}} N((3\theta^2)' \mid_{x=\theta})$$

Now check for algebraic ints of the forms

$$\alpha = \frac{1}{3}(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2), \lambda \in \{0, 1, 2\}$$

or

$$\alpha = \frac{1}{5}(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2), \lambda \in \{0, 1, 2, 3, 4\}$$

Regarding the second case, we find the trace and the norm.

$$N(\alpha) = \prod_{j=1}^{3} \sigma_j(\alpha) = \frac{\lambda_2^3 + 5\lambda_3^3}{25}$$

so we want

$$\lambda_2^3 + 5\lambda_3^3 \equiv 0 \mod 25$$

Suppose that $\lambda_2, \lambda_3 \neq 0 \mod 5$ This cannot be true, so we can rule out the 1/5 type since there are no lambdas that give an integer norm. And the same is true of 1/3 so it's basis is

$$\{1, \theta, \theta^2\}$$

and $\mathcal{O}_k = \mathbb{Z}[5^{1/3}]$.

Chapter 3 summary

Quadratic fields — almost done with except for degree 2/Q. That is $K = Q(\sqrt{d})$, d square free. Embeddings

$$\sigma_1 : 1 \to 1, \sqrt{d} \to \sqrt{d}$$

$$\sigma_2 : 1 \to 1, \sqrt{d} \to -\sqrt{d}$$

The norm is $a^2 - db^2$. The trace is $2a$. The number ring/discrimanent is (see earlier section)

Cyclotomic fields. Let

$$K = Q(\zeta), \zeta = e^{\frac{2\pi i}{n}}$$

odd prime nth root of unity. For this section assume $n = p$ prime. The minimal polynomial

$$\zeta(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \cdots + t + 1$$

so $[Q(\zeta) : Q] = p - 1$. Therefore there exists $p - 1$ embeddings.

$$\sigma_j(\zeta) = \zeta^j$$

$$\mathcal{O}_k = \mathbb{Z}[\zeta]$$

$$N(\zeta) = 1$$

$$N(\zeta^j) = 1$$

$$\text{Tr}(\zeta) = -1 = \text{Tr } (\zeta^j) = -1$$

$$N(1 - \zeta) = \prod_{k=1}^{p-1}(1 - \zeta^k)$$

which is the min poly at $t = 1$ or

$$N(1 - \zeta) = p$$

The discriminant of $Q(\zeta)$ is

$$(-1)^{\frac{p-1}{2}} p^{p-2}$$

Proof of theorem 2.18.

$$\zeta'(t) = \frac{pt^{p-1}(t-1) - (t^p - 1)1}{(t-1)^2} = \frac{-p\zeta^{p-1}}{1 - \zeta}$$

We plug into our formula to get the norm. Now the norm is multiplicative, so

$$(-1)^{\frac{(p-1)(p-2)}{2}} N(\frac{-p\zeta^{p-1}}{1 - \zeta}) = (-1)^{\frac{p-1}{2}} p^{p-2}$$

because $N(-p) = (-p)^{p-1}$,