Notes for Cryptography

Professor Brian Sittinger

2/8/16

1 HW2 Questions

See HW2.tex. Also, hw3 is supposedly harder.

2 Chapter 2

We're going through half of chapter 2. I should catch up on my reading.

2.1 Field Extensions

A Field is a commutative ring with multiplicative inverses. Let k be a field. Then L is a field extension of k iff L is a field containing k. For this course $k = \mathbb{Q}$ most of the time. For example $\mathbb{C}$ is a field extension of $\mathbb{R}$. $\mathbb{R}$ is a field extension of $\mathbb{Q}$. And $\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$ is a field extension of $\mathbb{Q}$. When L is a field extention of k, we write $L : k$. L is a Vector Space over k. So, we can discuss the "Dimension" called "the degree" of the field extension over k written $[L : k]$.

2.1.1 Examples

$$[\mathbb{Q}(i) : \mathbb{Q}] = 2$$

because $\mathbb{Q}(i)$ has basis $\{1, i\}$ over $\mathbb{Q}$.

2.2 Tower Law

Let

$$K \subseteq L \subseteq M$$

be a "tower" of 3 fields, or 3 fields such that

$$L : K, M : L$$

Then

$$[M : K] = [M : L] \cdot [L : K]$$

This is used in homework 3.

Suppose we wanted to find

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$$

we may now consider

$$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$$

and

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$$

Note: The minimal polynomial gives the degree of the extension. Be thorough.

Generally, we will concern ourselves with finite extensions, due to relevance. We define

$$L:K,\alpha\in L$$

1. If there exists a polynomial $p(t)\in K[t]$ such that $p(\alpha)=0$. Then α is algebraic over the base field K.

2. Otherwise, α is not algebraic but trancendental.

We'll let $K=\mathbb{Q}$ in this course. Examples of trancedental numbers are π and e. Consider

`https://en.wikipedia.org/wiki/Liouville_number`

So how many algebraic numbers and trancendental numbers over $\mathbb{Q}$ exist? There are countably many algebraic numbers, and uncountably many trancendentals. We can see this by first noting that $\mathbb{Q}$ is countable, and then noting that $\mathbb{C}$ is uncountable.

Suppose α is algebraic over K. Then the monic polynomial $p(K)$ of smallest degree for which $p(\alpha)=0$ is called the minimal polynomial of α over K.

Some interesting notes:

- The minimal polynomial is irreducible over K.

- Take $k=\mathbb{Q}$. Then we can clear "denominators" so that we have a minimal polynomial with coefficients in the integers

Let $L:K$ with $\alpha\in L$. Then α is algebraic over K is equivalent to saying that

$$[K(\alpha):K]<\infty$$

Moreover,

$$[K(\alpha):K]=\deg(\text{min poly of } a)$$

and

$$K(a)=K[a]$$

the difference in notations refers to the difference between a ring and a field. That is

$$K[a_1,a_2,\ldots,a_n]$$

is the smallest ring containing $a_1, \ldots, a_n$. This is in essence a set of polynomials in $a_1, \ldots, a_n$ with coefficients in K. Similarly,

$$K(a_1, \ldots, a_n)$$

is the smallest field containing $a_1, \ldots, a_n$. It is the set of rational functions in $a_1, \ldots, a_n$ with coefficients in K. What are rational functions? Similar to polynomials, it can be defined

$$k(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \mid f, g \in K[a_1, \ldots, a_n] \text{ and } g \neq 0 \right\}$$

Let d be a squarefree integer. Look at

$$\mathbb{Q}[\sqrt{d}]$$

Then

$$[Q\mathbb{Q}[\sqrt{d}] : \mathbb{Q}] = 2$$

because $x^2 = d$ is the minimum polynomial of $\sqrt{d}$ over $\mathbb{Q}$. And $\sqrt{d}$ is algebraic over $\mathbb{Q}$. Also,

$$\mathbb{Q}[\sqrt{d}] = \left\{ a \cdot 1 + b\sqrt{d} \mid a, b \in \mathbb{Q} \right\}$$

has basis $\{1, \sqrt{d}\}$. This is closed under addition and multiplication. Next, we note that

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$$

We show that the field is contained within the ring by using the conjugate, that is

$$\frac{1}{a_b\sqrt{d}} \cdot \frac{a - b\sqrt{d}}{a - b\sqrt{d}}$$

Now, $\mathbb{Q}[\sqrt{d}]$ is a quadratic number field. Look this up in more detail. Back to algebraic numbers and integers!

3 Algebraic Numbers and Integers

We define the set of all algebraic numbers over $\mathbb{Q}$ sometimes denoted $\mathbb{A}$ or $\bar{\mathbb{Q}}$. In the homework, we may show that

$$[\mathbb{A} : \mathbb{Q}] = \infty!!$$

where we count down by two for double factorial.

Note that $\mathbb{A}$ is a subfield of $\mathbb{C}$. Let $\alpha, \beta \in \mathbb{A}$. Then by the tower law

$$[p\mathbb{Q}(\alpha, \beta)] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

We are multiplying two finite extensions together, since β is algebraic over $\mathbb{Q}$ and so $\mathbb{Q}(\alpha)$ is too. Therefore $\mathbb{Q}(\alpha, \beta)$ is a finite extension over $\mathbb{Q}$ and so closure and inverses under addition and multiplication are guaranteed.

Now we define K as an algebraic number field over $\mathbb{Q}$ if K is a subfield of $\mathbb{C}$ and $[K, \mathbb{Q}]$ is finite. So, K is a subfield of $\mathbb{A}$ and $K = \mathbb{Q}(a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in K$. We can do better, though — we only need 1 generator! That is $K = \mathbb{Q}(\theta)$ for some $\theta \in \mathbb{A}$. See Theorem 2.2 from the book.

To find the professor's mailbox, look for a copy room past Chris, a guy with a computer.

Algebraic integers over the rationals are a zero of a monic polynomial in the integers.

Number Fields	Number Rings
$\bar{\mathbb{Q}}$ or $\mathbb{A}$	$\mathbb{B}$
$\mathbb{Q}(\theta) = K$	$\mathbb{Z}[\alpha] = \mathcal{O}$
$\mathbb{Q}$	$\mathbb{Z}$
Number Field Tower	Number Ring Tower

For example, if $k = \mathbb{Q}(i)$, then $\mathcal{O} = \mathbb{Z}[i]$.

4 Conjugates, norms and traces

This has a flavor of Galois theory to it. Theorem 2.4 from the book. Let $k = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. Then there are exactly n distinct embeddings $\sigma_j : K \to \mathbb{C}$ with $j = 1, \ldots, n$. Embeddings are one to one ring homomorphisms that fix $\mathbb{Q}$. That is $\sigma_j(q) = q \forall q \in \mathbb{Q}$. Moreover, the elements $\sigma_j(\theta) \equiv \theta_j$ for each $j = 1, \ldots, n$ are the distinct zeros in $\mathbb{C}$ of the minimal polynomials of θ over $\mathbb{Q}$. The elements $\theta_1, \ldots, \theta_n$ are the k-conjugates of θ.

4.1 Example

More about $K = \mathbb{Q}(\sqrt{d})$ where d is square free. Recall that the minimal polynomial is $x^2 - d$ with zeroes $\pm\sqrt{d}$. By our theorem, there exists $[\mathbb{Q}(\sqrt{(d)}) : \mathbb{Q}] = 2$ embeddings. And so

$$\sigma_1(1) = 1 \text{ and } \sigma_1(\sqrt{d}) = \sqrt{d}$$

So

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$$

So we see that this is the identity map.

Let us now consider σ_2 where

$$\sigma_2(1) = 1 \text{ and } \sigma_2(\sqrt{d}) = -\sqrt{d}$$

And so σ_2 is what we used to call “conjugation.”

4.2 Another Example

Let $K = \mathbb{Q}(6^{1/3})$. The minimum polynomial is $x^3 - 6$ with three roots $\sqrt{6}, \omega 6^{1/3}, \omega^2 6^{1/3}$ where $\omega = e^{\frac{2\pi}{3}}$ is a cube root of unity. By our theorem, there are 3 embeddings.

1. $\sigma_1(1) = 1$
2. $\sigma_1(6^{1/3}) = 6^{1/3}$
3. $\sigma_1(6^{2/3}) = 6^{2/3}$ Because it's a homomorphism.

And so σ_1 is the identity map.

$$\sigma_2(1) = 1, \sigma_2(6^{1/3}) = \omega 6^{1/3}, \sigma_2(6^{1/3}) = (\omega 6^{1/3})^2$$
$$\sigma_3(a + b6^{1/3} + c6^{2/3}) = a + b(\omega^2 6^{1/3}) + c(\omega^2 6^{1/3})^2$$

Let $K = \mathbb{Q}(\theta)$ of degree n over $\mathbb{Q}$, and $\{a_1, \ldots, a_n\}$ be a basis of K over $\mathbb{Q}$. We define the "discriminent"

$$\Delta[a_1, \ldots, a_n] = \{\det(\sigma_i(a_j))\}^2$$

We define the Trace of a denoted $\mathrm{Tr}(a)$ as

$$\mathrm{Tr}(a) = \sum_{j=1}^{n} = \sigma_j(a)$$

We define the Norm for $a \in K$ as

$$N(a) = \prod_{j=1}^{n} \sigma_j(a)$$

And so we note that $\Delta, \mathrm{Tr}, N \in \mathbb{Q}$. Moreover, if we replace K with $\mathcal{O}_k$, then $\Delta, \mathrm{Tr}, N \in \mathbb{Z}$.

Some other facts. The Trace is additive and the Norm is multiplicative.

We return now to $K = \mathbb{Q}[\sqrt{d}]$.

$$\mathrm{Tr}(a + b\sqrt{d}) = 2a$$

$$N(a + b\sqrt{d}) = a^2 - db^2$$

$$\Delta[1, \sqrt{d}] = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d$$