ALGEBRAIC NUMBER THEORY

LECTURE 3 SUPPLEMENTARY NOTES

Material covered: Sections 2.1 through 2.5 of textbook.

1. Section 2.1

Proof of Theorem 1, (b) $\Rightarrow$ (c): Once we have the system of equations,

$$(x \cdot I - C)y = 0$$

where $C = (a_{ij})$, we can multiply the matrix $x \cdot I - C$ by its adjoint, which results in the scalar matrix $d \cdot I = (det(x \cdot I - C))I$ multiplying y to give the zero vector. This implies $dy_i = 0$ for all i and then $d = 0$ as in the book.

Example. Let K be a number field. Then any $x \in K$ is algebraic over $\mathbb{Q}$. It satisfies a unique monic polynomial equation of smallest degree

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

with $a_i \in \mathbb{Q}$. If all the coefficients a_i are integers, we say that x in an algebraic integer. The ring of algebraic integers of K is called $\mathcal{O}_K$.

Example. The algebraic number $\sqrt{3}$ is an algebraic integer, since it satisfies $x^2 - 3 = 0$. But $(1 + \sqrt{3})/2$ is not an algebraic integer, since its minimal polynomial is $2x^2 - 2x - 1$. On the other hand the Golden ratio $(1 + \sqrt{5})/2$ is an algebraic integer. Its minimal polynomial is $x^2 - x - 1$.

Proof of Proposition 3: Here is an alternate proof of the first part: if B is integral over A and A is a field, then B is a field. Let $0 \neq b \in B$ satisfy the following equation of minimal degree over A:

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

We can assume that $a_0 \neq 0$ else we can factor out b and cancel it to get a lower degree, since B is an integral domain. Then we have

$$b(b^{n-1} + \cdots + a_1) = -a_0$$

so that $-a_0^{-1}(b^{n-1} + \cdots + a_1)$ is a multiplicative inverse for b.

2. Section 2.2

Example 2.2 is a special case of the *Gauss lemma*: Every UFD (unique factorization domain, or factorial ring, in Samuel's terminology) is integrally closed. The proof is the same as in the book, word for word.

3. Section 2.3

Example. Here is an example where $K \subset R, x \in R$ is integral over K but $k[x]$ is not an integral domain (or equivalently a field, in this situation).

Let $R \subset M_2(K)$ (the 2×2 matrices over K) be $K[x]$, where

$$x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and $K \hookrightarrow M_2(K)$ as scalar matrices. The minimal polynomial of x is easily seen to be $X^2 - 1$, which is not irreducible. Here $K[x]$ is a direct sum of two copies of K, as an algebra over K.

4. Section 2.4

We say a field K is *perfect* if every algebraic extension of K is separable over K. In other words, any monic irreducible polynomial over K splits over $\overline{K}$ into a product of distinct monic linear factors.

Example. Any field of characteristic 0, or any finite field, is perfect.

Example. An example of a non-perfect field is $K = \mathbb{F}_p(T)$. The polynomial $X^p - T$ is irreducible over K, but over the extension $K(T^{1/p}) = \mathbb{F}_p(T^{1/p})$, it splits as $(X - T^{1/p})^p$, so it has multiple roots.

Theorem 1 (Theorem of primitive element)**.** *Let K be a perfect field, and L/K a finite extension. Then $\exists x \in L$ such that $L = K[x]$.*

5. Section 2.5

A *number field* is a finite extension of $\mathbb{Q}$. Number fields are labelled by their degree: quadratic if they have degree 2 over $\mathbb{Q}$, cubic, quartic, quintic and so on. If K is a number field, we let $\mathcal{O}_K$ be the ring of integers of K, which is the integral closure of $\mathbb{Z}$ in K.

Note that for quadratic fields, we see by the explicit description of $\mathcal{O}_K$ that it is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$. In fact this is true for any number field. A subring of $\mathcal{O}_K$ of rank $[K : \mathbb{Q}]$ over $\mathbb{Z}$ is called an *order*.

6. GP example

```
f = x^3 + 3*x + 1;
F = bnfinit(f);
charpoly(Mod(x^2,f));
```

The last command computes the characteristic polynomial of α^2, where α is a root of f.

```
a = sqrt(3) + sqrt(2)
algdep(a,4)
```

This command produces a best possible approximation to a minimal polynomial of the specified degree. To set the precision in gp, use

```
default(realprecision,100);
```

18.786 Topics in Algebraic Number Theory
Spring 2010