ALGEBRAIC NUMBER THEORY

LECTURE 4 SUPPLEMENTARY NOTES

Material covered: Sections 2.6 through 2.9 of textbook.

I followed the book pretty closely in this lecture, so only a few comments.
Wherever Samuel states a theorem with the assumption that a field has characteristic zero or is finite, we can generalize to the field being perfect.

1. Section 2.6

To compute the determinant of the matrix

$$\begin{pmatrix} X & 0 & \dots & a_0 \\ -1 & X & \dots & a_1 \\ \dots & -1 & X & a_{n-2} \\ \dots & 0 & -1 & X + a_{n-1} \end{pmatrix}$$

first add X times the bottom row to the second last row, then X times the second last row to the third last, and so on. We get

$$\begin{pmatrix} 0 & 0 & \dots & X^n + a_{n-1}X + \cdots + a_1 X + a_0 \\ -1 & 0 & \dots & X^{n-1} + a_{n-1}X^{n-2} + \cdots + a_1 \\ \dots & -1 & 0 & X^2 + a_{n-1}X + a_{n-2} \\ \dots & 0 & -1 & X + a_{n-1} \end{pmatrix}$$

Now Laplace expand along the first column, and so on, to get that the determinant is $f(X)$, the minimal polynomial of x, which is the top right entry of the above matrix.

Example. Suppose $A \subset B \subset C$ are rings, such that B is a free module over A and C is a free module over B. Let $x \in C$. Show that

$$\text{charpoly}_{B[X]/A[X]}\text{charpoly}_{C/B}(x) = \text{charpoly}_{C/A}(x)$$

Note that this is using that $B[X]$ is a free $A[X]$ module. In particular, check that this implies that traces and norms of elements are transitive.

2. Appendix: the fundamental theorem of algebra

Let's see a slightly different proof from that in the book (it's from Grillet's Abstract Algebra).

We will use that any polynomial of odd degree over $\mathbb{R}$ has a real root, and that any element of $\mathbb{C}$ has a square root. These are elementary to see: for the first look at the values of $f(x)$ as $x \to +\infty$ and as $x \to -\infty$, and observe that there must be a sign change in between. For the second, we can write $z = re^{i\theta}$ and then $\sqrt{r}e^{i\theta/2}$ is a square root.

Now if K is an extension of $\mathbb{R}$ of finite odd degree, it must equal $\mathbb{R}$ (for there is a primitive element α, and its minimal polynomial is of odd degree and so has a root in $\mathbb{R}$, so $\mathbb{R}[\alpha] \cong \mathbb{R}$.

Let L be a finite extension of $\mathbb{C}$, which we can assume is Galois over $\mathbb{R}$ (else replace L by its Galois or normal closure). Then let $G = \mathrm{Gal}\,(L/\mathbb{R})$ be its Galois group. If G_2 is a 2-Sylow subgroup of G, then the fixed field of G_2 is an odd degree extension of $\mathbb{R}$, so it must equal $\mathbb{R}$. So G is a 2-group (i.e. it has order a power of 2), and so is the subgroup $\mathrm{Gal}\,(L/\mathbb{C})$. By the Sylow theorems, if $\mathrm{Gal}\,(L/\mathbb{C})$ is non-trivial, it has a subgroup of index 2, whose fixed field is a quadratic extension of $\mathbb{C}$, which is impossible. So $L = \mathbb{C}$.