NAP 2018, NOTES ON CLASS #6, 16 MAY, 2018

• We proved **Proposition 1.20: Multiplicativity of Degrees** (of extension fields). We added just a couple of details to the proof in the book, which is actually rather detailed. We said (many times, and will say many times again) that one should always draw a lattice diagram (graph) showing intermediate fields at vertices, and labeling edges with degrees.

• We proved **Lemma 1.23:** A domain R containing a field F is a field if R is finite dimensional as a vector space over F.

This shows that $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is a field. (Earlier we showed $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is spanned by $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ as a $\mathbb{Q}$-vector space.) Therefore $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

• For an element α of an extension field K of F, one says that α is *algebraic over* F provided there is a *non-zero* polynomial $f(X)) \in F[X]$ having α as a root. If no such polynomial exists, then α is *transcendental over* F.

• The exponential base e is transcendental over $\mathbb{Q}$, and the proof is not too hard, roughly speaking, because the power series expansion of e is so sparse. Also, π is transcendental, but the proof is much harder. It is not known whether or not $\frac{e}{\pi}$ is transcendental. In fact, it's not even known whether or not $\frac{e}{\pi} \in \mathbb{Q}$!

• For an element α in a field extension K of F, we pointed out that $F[\alpha] \cong F[X]$ if α is transcendental over F, and hence that $F[\alpha]$ is *properly* contained in $F(\alpha)$. If α is algebraic over F, then $F[\alpha] = F(\alpha)$, by FATSAE (below).

We proved various characterizations of the *minimal polynomial* of an algebraic element:

• **Proposition 1.27$\frac{1}{4}$:** Let α be an element of a field extension K of F with α algebraic over F. Let I be the kernel of the "evaluation" homomorphism $F[X] \to F[\alpha]$ taking $g(X)$ to $g(\alpha)$. Let $p(X)$ be a monic polynomial in $F[X]$. These conditions on $p(X) \in F[X]$ are equivalent:

(a) $p(\alpha) = 0$, and $p(X)$ has least degree among all *non-zero* polynomials $f(X) \in F[X]$ such that $f(\alpha) = 0$.
(b) $I = p(X)F[X] = (p(X))$, that is, $p(X)$ generates the ideal I.
(c) $p(\alpha) = 0$ and $p(X)$ is irreducible.

Well, maybe we didn't include (c) among these conditions, but we will do so in our last class, on Thursday, 17 May.

• We proved what we call the "Fundamental Theorem on Simple Algebra Extensions (FTSAE), aka Theorem 1.27$\frac{1}{2}$). It covers various things in the book (e.g., "stem fields") that seem to be a bit scattered.

• **Theorem 1.27$\frac{1}{2}$ FTSAE**: Let α be an element of an extension field K of F. Assume α is algebraic over F, and let $p(X)$ be a monic polynomial such that (i) $p(\alpha) = 0$ and (ii) $p(X)$ has least degree among all *non-zero* polynomials having α as a root. Put $n = \deg f(X)$. Then:

(1) $p(X)$ is unique (and is called the *minimal polynomial* of α over F).
(2) $p(X)$ is irreducible in $F[X]$.
(3) The set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $F[\alpha]$ as a vector space over F.
(4) For a polynomial $g(X) \in F[X]$, we have $g(\alpha) = 0 \iff p(X) \mid g(X)$.
(5) $F[\alpha]$ is a field, and so $F[\alpha] = F(\alpha)$.
(6) $[F(\alpha) : F] = n$.

Of course item (5) follows from Lemma 1.23, but we gave another (constructive) proof, using the fact that the GCD of two gadgets is a linear combination of the gadgets. Thus one can find inverses constructively, using the Euclidean Algorithm.