MAT 632 — HOMEWORK 7

DUE ON WEDNESDAY, 2 APRIL

1. Let K/F be a field extension of degree n, and $\alpha \in K$. Prove that multiplication by α is an F-linear transformation of (the F-vector space) K. Show that this implies that K is isomorphic to a subring of the ring of $n \times n$ matrices over F, so that the (noncommutative) ring $M_n(F)$ contains a copy of *every* field extension of F of degree $\le n$.

2. Let $F(\alpha)$ be an extension of a field F with $[F(\alpha):F]$ odd. Prove that $F(\alpha^2) = F(\alpha)$.

3. Find the minimal polynomial for α over F:

(a) $\alpha = \sqrt{5+3\sqrt{2}}, \quad F = \mathbb{Q}$

(b) $\alpha = 1+(\sqrt[3]{2})^2, \quad F = \mathbb{Q}$

(c) $\alpha = \sqrt{3}+\sqrt{5}, \quad F = \mathbb{Q}$

(d) $\alpha = \sqrt{3}+\sqrt{5}, \quad F = \mathbb{Q}(\sqrt{3})$

(e) $\alpha = \sqrt{3}+\sqrt{5}, \quad F = \mathbb{Q}(\sqrt{15})$

(You may assume that $\sqrt{n} \notin \mathbb{Q}$ for non-square integers n.)

4. Find a splitting field F for $f(x)$ over $\mathbb{Q}$, and determine $[F:\mathbb{Q}]$

(a) $f(x) = x^4+1$

(b) $f(x) = x^4+x^2+1$ (Hint: complete the square.)

5. Give examples of three polynomials $f_1(x), f_2(x), f_6(x) \in \mathbb{Q}[x]$ of degree 3 such that the splitting field of f_i has degree i over $\mathbb{Q}$.

6. Give another, easier, proof of the the Lemma from class about finite subgroups of $F^\times$, along the following lines: use the FToFGAG, induction on the number of cyclic summands, the fact that $\mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ is cyclic if $\gcd(a,b) = 1$, $\operatorname{lcm}(a_1,\ldots,a_n) < a_1 a_2 \ldots a_n$ if $\gcd(a_1,a_2) > 1$, and $g^{|G|} = 1$ for every $g \in G$.

7. (a) Let p be an odd prime. Prove that exactly half the elements of $\mathbb{F}_p^\times$ are squares, and that the product of any two nonsquares is a square. (Hint: use the Lemma above.)

(b) Write down $\operatorname{Irr}_{\mathbb{Q}}(\sqrt{2}+\sqrt{3})$ (and justify).

(c) Prove that $\operatorname{Irr}_{\mathbb{Q}}(\sqrt{2}+\sqrt{3})$ is reducible mod p for every prime p.

8. Let F be a field of characteristic p, with prime subfield $\mathbb{F}_p$. Prove that $F/\mathbb{F}_p$ is a simple extension, i.e. there is an element $\alpha \in F$ so that $F = \mathbb{F}_p(\alpha)$. (Lemma again.) Conclude that every finite field has order p^n for some p, n.