Homework 1

due on Thursday, February 21

Read Chapters 2 and 3 in Milne's book. Study Chapter 13 in Dummit and Foote Solve the following problems.

Problem 1. Let F be the algebraic closure of $\mathbb{Q}$ in $\mathbb{R}$. Prove that $\mathrm{Aut}(F/\mathbb{Q})$ is trivial. Hint: Show first that $a \in F$ is positive iff a is a square in F.

Problem 2. Let K be a field and let $K(u)$ be an extension of K such that u is transcendental over K (we call $K(u)$ a simple transcendental extension of K).

a) Let $f(x), g(x)$ be relatively prime polynomials in $K[x]$ (at lest one of which is not constant). Prove that the polynomial $ug(x) - f(x)$ is irreducible in $K(u)[x]$.

b) Let $a \in K(u)$, $a \notin K$. Note that there are relatively prime polynomials f, g in $K[x]$ such that $a = f(u)/g(u)$. Prove that $[K(u) : K(a)] = \max(\deg f, \deg g)$.

c) Let $A = \left(\begin{smallmatrix} p & q \\ s & t \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ be an invertible 2×2 matrix. Prove that there is a unique automorphisms τ_A of $K(u)/K$ such that $\tau_A(u) = (pu+q)/(su+t)$.

d) Prove that the map $A \mapsto \tau_{A^{-1}}$ is a surjective homomoirphism from $\mathrm{GL}_2(K)$ to $\mathrm{Aut}(K(u)/K)$ whose kernel consists of scalar matrices. Conclude that $\mathrm{Aut}(K(u)/K)$ is isomorphic to $\mathrm{PGL}_2(K)$.

e) Prove that if Γ is an infinite subgroup of $\mathrm{Aut}(K(u)/K)$ then $K(u)^{\Gamma} = K$.

f) Let σ, τ be the automorphisms in $\mathrm{Aut}(K(u)/K)$ determined by $\sigma(u) = 1/u$ and $\tau(u) = 1 - u$. Prove that the subgroup G of $\mathrm{Aut}(K(u)/K)$ generated by σ and τ is isomorphic to the symmetric group S_3. Prove that $K(u)^G = K((u^2 - u + 1)^3/u^2(u-1)^2)$.

Problem 3. a) Let $L = K(a)$ be a simple algebraic extension of K. Let p be the minimal polynomial of a over K. Suppose that M is a subfield of L containing K. Let p_M be the minimal plynomial of a over M. Prove that M is generated over K by the coefficients of p_M.

b) Let K be infinite. Prove that a finite extension L/K is simple if and only if the set of all subfields of L which contain K is finite. (Hint. For $\Rightarrow$ use a) and the fact that a polynomial over a field has a finite number of monic divisors. For $\Leftarrow$, do this first assuming that $L = K(a,b)$). (The result is also true for K finite, but requires different method).

c) Let $L = K(x,y)$ be the field of rational functions in two variables over a field K of characteristic $p > 0$. Prove that $[K(x,y) : K(x^p, y^p)] = p^2$. Prove also that every element of L is either of degree p or of degree 1 over $M = K(x^p, y^p)$. Conclude that L/M is not simple.

Problem 4. Let $a = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ (where we take positive square roots to be concrete). Let $L = \mathbb{Q}(a)$.

a) Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$. Observe that its Galois group has 2 elements: 1 and ϕ. Let $u = a^2$. Compute $u\phi(u)$. Use this to prove that u is not a square in the field $M = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Conclude that $L/\mathbb{Q}$ has degree 8.

b) Prove that the roots of the minimal polynomial of a over $\mathbb{Q}$ are the 8 numbers $\pm\sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})}$. Find the minimal polynomial.

c) Let $b = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$. Prove that $ab \in M$ and conclude that $b \in L$. Use similar argument to prove that L is a splitting field of the minimal polynomial of a. Conclude that $L/\mathbb{Q}$ is Galois. Let $\Gamma = \mathrm{Gal}(L/\mathbb{Q})$.

d) Prove that there are σ, τ in Γ such that $\sigma(a) = b$ and $\tau(a) = \sqrt{(2+\sqrt{2})(3-\sqrt{3})}$. Prove that $\sigma(b) = -a$. Conclude that σ has order 4. Prove similarly that τ has order 4.

e) Prove that σ and τ generate Γ. Prove that $\sigma^2 = \tau^2$ and $\sigma\tau = \tau\sigma^{-1}$. Conclude that Γ is isomorphic to the quaternion group of order 8.

Problem 5. Let $\mathcal{P}$ be a property of algebraic field extensions L/K. Consider the following statements about $\mathcal{P}$:

a) If $K \subseteq L \subseteq M$ are fields and L/K and M/L have property $\mathcal{P}$ then M/K has property $\mathcal{P}$.

b) If $K \subseteq L \subseteq M$ are fields and M/K has property $\mathcal{P}$ then M/L has property $\mathcal{P}$.

c) If $K \subseteq L \subseteq M$ are fields and M/K has property $\mathcal{P}$ then L/K has property $\mathcal{P}$.

d) If L_1/K and L_2/K are extensions contained in a field F and both have ptoperty $\mathcal{P}$ then L_1L_2/K has property $\mathcal{P}$.

e) If L_1/K and L_2/K are extensions contained in a field F and both have property $\mathcal{P}$ then $(L_1 \cap L_2)/K$ has property $\mathcal{P}$.

f) If L/K and M/K are extensions contained in a field F and L/K has property $\mathcal{P}$ then LM/M has property $\mathcal{P}$.

For each of the following properties $\mathcal{P}$: normal, separable, Galois, purely inseparable, and simple, and for each of the statements a)-f), either prove that the statement is true for $\mathcal{P}$ or give a counterexample.