Math 210B. Homework 1

1. Prove that $f = X^3+3X+1$ is irreducible over $\mathbf{Q}$. Letting α be a root of f in an extension, use that f vanishes at α and $f(X-1)$ vanishes at $\alpha+1$ to express $1/\alpha$ and $1/(\alpha+1)$ as quadratic polynomials in α with $\mathbf{Q}$-coefficients (as must be possible since $\mathbf{Q}[\alpha] = \mathbf{Q}(\alpha)$).

2. Consider $f \in k[T, X]$ that is not divisible by any non-constant elements of $k[T]$ or $k[X]$. Prove that f is irreducible when viewed in $k(X)[T]$ if and only if it is irreducible when viewed in $k(T)[X]$. Deduce that $X^n - T$ is irreducible in $k(T)[X]$ for any integer $n > 0$.

3. For a prime p, let $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ denote the field with p elements. Consider the field $L = \mathbf{F}_p(X, Y)$ and its subfield $k = \mathbf{F}_p(X^p, Y^p)$. Let $x = X^p, y = Y^p$ in k.

(i) Prove L/k is a splitting field of $(T^p - x)(T^p - y)$ and $[L : k] = p^2$.

(ii) Prove every $\alpha \in L$ satisfies $\alpha^p \in k$, and deduce L/k does *not* admit a primitive element.

(iii) Construct *infinitely many* distinct subfields of L of degree p over k.

4. (i) For a commutative ring R and R-algebras A and A', prove that $A \otimes_R A'$ has a unique R-algebra structure with identity $1 \otimes 1'$ such that $(a_1 \otimes a_1')(a_2 \otimes a_2') = (a_1a_2) \otimes (a_1'a_2')$. Also prove $A \otimes_R (R[X_1, \dots, X_n]) \simeq A[X_1, \dots, X_n]$ via $1 \otimes X_j \mapsto X_j$ and $a \otimes 1 \mapsto a$.

(ii) If K, K' are extensions of a field k, construct an extension field F/k into which K and K' embed as subfields *over* k (hint: show $K \otimes_k K' \neq 0$, and quotient by a maximal ideal). Deduce that any two fields with the same characteristic are subfields of a common field.

5. Read Ch. VIII, §1 in Lang's *Algebra* concerning transcendence bases and transcendence degree (feel free to focus on finitely generated extensions, all we need). Prove that if $K'/K/k$ is a tower of finitely generated extensions with $n = \mathrm{trdeg}(K/k)$ and $m = \mathrm{trdeg}(K'/K)$ then $\mathrm{trdeg}(K'/k) = n + m$. (Hint: first treat the case $n = 0$).

6. Let k be a field with $\mathrm{char}(k) = p > 0$, and let $h \in k[X]$ be *monic* irreducible.

(i) Prove $h(X^p)$ is irreducible if and only if $h \notin k^p[X]$, in which case $h(X^{p^r})$ is irreducible for all $r \geq 1$. (Hint: since $h(X^p) = \prod f_j^{e_j}$ with $e_j \geq 1$ and pairwise distinct monic irreducible f_j, analyze possibilities depending on if $p|e_j$ or $f_j \in k[X^p]$.) Deduce that if $a \in k - k^p$ then $X^{p^r} - a$ is irreducible in $k[X]$ with a unique root in a splitting field for all $r \geq 1$, so $k = k^p$ when k is perfect, and that if k is imperfect then every *finite* extension k'/k is imperfect.

(ii) Let K/κ be a finitely generated *non-algebraic* extension (i.e., positive transcendence degree) with $\mathrm{char}(\kappa) = p > 0$. Using the end of (i), prove that K is *always* imperfect.

7. Let k be a field, and A a nonzero commutative k-algebra with $\dim_k A < \infty$.

(i) Let $\alpha_1, \dots, \alpha_r$ be a finite generating set for A as a k-algebra (e.g., a k-basis). Show that each α_i satisfies $f_i(\alpha_i) = 0$ for a (not necessarily irreducible!) monic $f_i \in k[X]$.

(ii) Let F/k be a splitting field for $f := \prod f_i$. Show for $\mathfrak{m} \in \mathrm{Max}(A)$ that a splitting field of f over $A/\mathfrak{m}$ is *also* a splitting field for f over k, and deduce that there exists a k-embedding $A/\mathfrak{m} \hookrightarrow F$. But prove there are only *finitely many* k-algebra maps $A \to F$, so $\mathrm{Max}(A)$ is finite! (Beware F/k may have infinitely many intermediate fields; see Exercise 3(iii).)

(iii) The handout on finite-dimensional algebras shows $\mathfrak{m}A_{\mathfrak{m}}$ is nilpotent for each maximal ideal $\mathfrak{m}$ of A. Enumerating the maximal ideals as $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ by the finiteness proved in (ii), prove that $I := \bigcap \mathfrak{m}_i = \prod \mathfrak{m}_i$ is nilpotent in A, say $I^N = 0$. Using the equality $A = A/I^N$, deduce that $A \to \prod_i A_{\mathfrak{m}_i}$ is an isomorphism. (Hint: Chinese Remainder Theorem for pairwise comaximal ideals.)