Math 55a, Fall 2004

10 th Assignment, due November 30

1. Recall the two problems of the last assignment. This problem involves the notions of monic polynomial – a non-constant polynomial having leading coefficient 1 – and of irreducible polynomial – a non-constant polynomial that is not divisible by any non-costant polynomial of strictly lower degree. Let L be a field, $K \subset L$ a subfield. For $a \in L$, $K[a]$ shall denote the smallest *subring* of L containing K and a, and $K(a)$ the smallest *subfield* with this property. Prove all of the following statements:

a) The map $p \mapsto p(a)$ defines a surjective ring homomorphism from $K[X]$ to $K[a]$.

b) $K[a] = K(a)$ only if a is algebraic over K.

c) If a is algebraic over K, there exists a unique monic irreducible (as element of K[X]) polynomial $p \in K[X]$ with $p(a) = 0$.

d) Suppose p, $q \in K[X]$ are relatively prime (i.e., they are non-zero and have no common non-constant divisor). Then there exist $r, s \in K[X]$, such that $rp+sq = 1$.

e) Suppose that a is algebraic over K, and let $p \in K[X]$ be the monic irreducible polynomial whose existence was asserted in c). Then $K(a) = K[a]$, and the degree of $K(a)$ over K is equal to the degree of the polynomial p.

f) The polynomial $X^3 - 2$ is irreducible in $\mathbb{Q}[X]$.

g) It is impossible to "double the cube by ruler and compass" – in other words, it is impossible to construct, with a ruler and compass construction, the point $(\alpha, 0)$, where α denotes the cube root of 2, from the two points $(0, 0)$, $(1, 0)$.

h) It is impossible to "square the circle by ruler and compass"; in doing this problem, you may assume as known the fact that π is a transcendental number (i.e., it is not algebraic over $\mathbb{Q}$).

2. Let K be a field, $p \in K[X]$ an irreducible polynomial of degree at least two. By definition, an extension field L of K is a field L which contains K as subfield. A splitting field for p is an extension field L of K, such that p splits into a product of linear factors in $L[X]$, and such that L is generated over K by the roots of p. Prove the following statements:

a) There exists an extension field L of K, and an element $\alpha \in L$, such that $p(\alpha) = 0$ and $L = K[\alpha]$ (hint: $L = K[X]/I$, for an appropriately chosen maximal ideal $I \subset K[X]$).

b) Suppose L_1 , L_2 are two field extensions of K, with $L_1 = K[\alpha_1]$, $L_2 = K[\alpha_2]$ for $\alpha_1 \in L_1$, $\alpha_2 \in L_2$, and $p(\alpha_1) = 0$ in L_1 , $p(\alpha_2) = 0$ in L_2 . Then there exists a unique isomorphism of fields $\phi : L_1 \xrightarrow{\sim} L_2$, such that $\phi(a) = a$ for any $a \in K$ and $\phi(\alpha_1) = \alpha_2$.

c) There exists a splitting field for p (hint: use 1) inductively).

d) Any two splitting fields for p are isomorphic over K – i.e., there exists an isomorphism between them which is the identity map on K.

3. Let V be a vector space over some field K. A *projection operator* on V is a linear transformation $p : V \to V$ such that $p^2 = p$. If $T : V \to V$ is some other linear transformation, one calls a subspace $W \subset V$ T-*stable* or T-*invariant* if $T(W) \subset W$. Show:

a) If p is a projection operator, then so is $1_V - p$.

b) If p is a projection operator, $V = \mathrm{Ker}\ p \oplus \mathrm{Im}\ p$.

c) Let W_1, W_2 be subspaces of V with $V = W_1 \oplus W_2$. There exists a uniquely determined projection operator $p : V \to V$, such that $W_1 = \mathrm{Im}\ p$, $W_2 = \mathrm{Ker}\ p$.

d) Let $V = W_1 \oplus W_2$ and $p : V \to V$ be as in c), and let $T : V \to V$ be a linear transformation. Then W_1 and W_2 are both T-stable if and only if p and T commute – i.e., if and only if $p \circ T = T \circ p$.