Math 55a, Fall 2004

Tenth Assignment, Solutions
Adapted from Andrew Cotton and George Lee

Problem 1.

(a)

Claim 1. *Fix $a \in L$ and let $\mathbb{K} = \{p(a) \mid p \in K[X]\}$. Then $K[a] = \mathbb{K}$.*

Proof: Given two elements $x, y \in \mathbb{K}$, they can be written in the form

$$x = \sum_{i=0}^{m} k_i^{(1)} a^i \quad \text{and} \quad y = \sum_{i=0}^{n} k_i^{(2)} a^i,$$

where m, n are integers and the $k_i^{(j)}$ are in K. (For $i > m$, we let $k_i^{(1)} = 0$; for $i > n$, we let $k_i^{(2)} = 0$.) Then

$$x + y = \sum_{i=0}^{\max(m,n)} (k_i^{(1)} + k_i^{(2)}) a^i,$$

$$-x = \sum_{i=0}^{m} (-k_i^{(1)}) a^i,$$

$$x \cdot y = \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} k_j^{(1)} k_{i-j}^{(2)} \right) a^i,$$

so $\mathbb{K}$ is closed under addition, the additive inverse, and multiplication; thus, it is a subring of L. And it contains any $k \in K$ (take the constant polynomial k, evaluated anywhere) and it contains a (take the polynomial x, evaluated at a).

Now look at any subring of L containing K and a. Since it is closed under multiplication, it contains $k_i a^i$ for any nonnegative integer i and any element $k_i \in K$. And since it closed under addition, it contains the finite sum $\sum_{i=0}^{m} k_i a^i$ of any such elements. Thus any such subring contains $\mathbb{K}$; and therefore, $\mathbb{K}$ is indeed the smallest subring of L containing both K and a. ∎

The claim immediately implies that the given map ϕ is surjective. And it is clearly a ring homomorphism; given polynomials $p = \sum_{i=0}^{m} p_i X^i$

and $q = \sum_{i=0}^{n} q_i X^i$ (again letting p_i and q_i equal 0 for large enough i), we have

$$\begin{aligned} \phi(p+q) &= \phi\left(\sum_{i=0}^{\max(m,n)} (p_i+q_i)X^i\right) = \sum_{i=0}^{\max(m,n)} (p_i+q_i)a^i \\ &= \sum_{i=0}^{m} p_i a^i + \sum_{i=0}^{n} q_i a^i = \phi(p)+\phi(q), \end{aligned}$$

and similarly $\phi(p \cdot q) = \phi(p) \cdot \phi(q)$.

(b) Suppose that $K(a) = K[a]$. If $a = 0$ then it is algebraic over K; otherwise, since $K[a]$ is a field, a has a multiplicative inverse $\sum_{i=0}^{m} k_i a^i$. Then

$$\sum_{i=0}^{m} k_i a^{i+1} - 1 = a \sum_{i=0}^{m} k_i a^i - 1$$

is a nonconstant polynomial in a equal to 0, so a is algebraic over K.

(c) Let $I = \{q \in K[X] \mid q(a) = 0\}$. This is an ideal because for $q_1, q_2 \in I$, $r_1, r_2 \in K[X]$ we have (defining ϕ as in (a))

$$\begin{aligned} (q_1r_1 + q_2r_2)(a) &= \phi(q_1r_1 + q_2r_2) = \phi(q_1)\phi(r_1) + \phi(q_2)\phi(r_2) \\ &= q_1(a)r_1(a) + q_2(a)r_2(a) = 0. \end{aligned}$$

Because $K[X]$ is a principal ideal domain, we have $I = (d)$ for some $d \in K[X]$. Because a is algebraic, I is nonempty and $d \neq 0$. Dividing d by its leading coefficient yields a monic polynomial p with $I = (p)$.

Any nonzero polynomial in I is a multiple of p and hence its degree is at least $\deg p$. (We use this fact again in later parts.) If we could write $p = qr$ for nonconstant polynomials $q, r \in K[X]$, then $p(a) = q(a)r(a)$ (from part (a)) so either $q(a) = 0$ or $r(a) = 0$. But then we would have a nonzero polynomial with root a and degree *smaller* than $\deg p$, a contradiction. Therefore, p is irreducible.

Now suppose we had another monic irreducible polynomial $\tilde{p}$ with root a. Then $\tilde{p}$ is a multiple of p, but because it is reducible it must be p multiplied by some constant. Because both $\tilde{p}$ and p are monic, this constant must be 1. Therefore we must have $\tilde{p} = p$, and there is exactly *one* monic irreducible with root a.

(d) It is easy to verify that $\{pr + qs \mid r, s \in K[X]\}$ is an ideal (actually, it is the ideal generated by p and q). Since $K[X]$ is a PID, it equals (d) for some d. Then $d \mid p$ and $d \mid q$, and so d is a constant. Therefore,

$1 = dd^{-1} \in dK[X] = (d) = \{pr + qs \mid r, s \in K[X]\}$, and $pr + qs = 1$ for some r, s.

(e) Suppose that if some polynomial q has a nonconstant common divisor d with p. Assume without loss of generality that d is monic. Since p is irreducible, we must have $d = p$. So $p \mid q$, $q \in I$, and $q(a) = 0$. Taking the contrapositive of this result, we find that if $q \in K[X]$ has root a, then q is relatively prime to p.

Now suppose that we have a nonzero $t \in K[a]$. By (a), we can write $t = q(a)$ for some polynomial $q \in K[X]$. And since $t \neq 0$, from our above observation p and q must be relatively prime. So from (d) we can find $r, s \in K[X]$ such that

$$rp + sq = 1.$$

Then

$$1 = (rp + sq)(a) = r(a)p(a) + s(a)q(a) = 0 + s(a)q(a),$$

so $t^{-1} = s(a) \in K[a]$. Therefore $K[a]$ is closed under the multiplicative inverse, and it is a field. Thus, $K(a) \subset K[a]$. And since $K(a)$ is a ring containing K and a, we also have $K(a) \supset K[a]$. So $K(a) = K[a]$, as desired.

Now, say that $p = \sum_{i=0}^{m} p_i X^i$ has degree m with $k_m = 1$; we claim that $B = \{1, a, \ldots, a^{m-1}\}$ is an m-element basis.

As observed in part (c), p has minimal degree among nonzero polynomials with root a. Thus if $\sum_{i=0}^{m-1} k_i a^i = 0$, then $\sum_{i=0}^{m-1} k_i X^i$ is a polynomial with root a; since its degree is less than n, it must be the zero polynomial and $k_0 = k_1 = \cdots = k_{m-1} = 0$. Therefore the elements of B are linearly independent.

Next, for positive integers n let $\mathbb{S}_n$ denote the set $\operatorname{span}\{1, a, \ldots, a^n\}$. Recall that if $x \in \operatorname{span}(S)$, then $\operatorname{span}(S) = \operatorname{span}(S \cup \{x\})$. Then for $n \geq m$, since we have $a^n = a^m \cdot a^{n-m} = \sum_{i=0}^{m-1} -p_i a^{i+n-m} \in \mathbb{S}_{n-1}$, we know that $\mathbb{S}_{n-1} = \mathbb{S}_n$. Thus $\mathbb{S}_{m-1} = \mathbb{S}_m = \mathbb{S}_{m+1} = \cdots = \mathbb{S}_n$ for all $n \geq m$.

So suppose we have $x \in K(a)$; then we can write $x = \sum_{i=0}^{n} k_i a^i$ for coefficients $k_i \in K$. If $n \leq m-1$ then clearly $x \in \mathbb{S}_{m-1}$; otherwise, $x \in \mathbb{S}_n = \mathbb{S}_{m-1}$ so $\mathbb{S}_{m-1}$ equals all of $K(a)$.

(Here is the argument again, informally. We can write a^m as a linear combination of "smaller" terms $1, a^1, \ldots, a^{m-1}$. Then given any polynomial in a, if its degree is at least m we can write its leading term as a linear combination of smaller (exponent-wise) terms. Repeating this construction, we can eventually write this number as a linear combination of elements in B.)

Therefore B spans $K(a)$ and its elements are linearly independent; so it is a basis, and $[K(a):K] = |B| = m$, as desired.

(f) If X^3-2 could be written as a product of two nonconstant polynomials p and q in $\mathbb{Q}[X]$, then one (say, p) has degree one and the other has degree two. Then p has some root $a \in \mathbb{Q}$; so $(X^3-2)(a) = p(a)q(a) = 0$. But $X^3 - 2$ has no rational roots, a contradiction. To show $X^3 - 2$ has no rational roots, suppose that $(\frac{m}{n})^3 = 2$. Then $m^3 = 2n^3$, but 3 divides the left hand side a total of 3α times and the right hand side a total of $3\beta + 1$ times for some integers α, β. Then $1 = 3(\alpha - \beta)$ is divisible by 3, which is impossible.

(g) Since $X^3 - 2$ is a monic irreducible with root $\sqrt[3]{2}$, from (e) the field $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}]$ has dimension 3 over $\mathbb{Q}$. Now, look at the smallest subfield of $\mathbb{R}$ containing both coordinates of $p = (\sqrt[3]{2}, 0)$. As in the last homework assignment, it must contain $\mathbb{Q}$, so it actually equals $\mathbb{Q}(\sqrt[3]{2})$. Thus $\mathbb{Q}(\{p\})$ has degree 3 over $\mathbb{Q}$; and since 3 is not a power of 2, from the last assignment we can't construct p with ruler and compass.

(h) Suppose by way of contradiction we could square the circle. Then starting with the points $(0,0)$ and $(1,0)$, we can construct the circle centered at $(1,0)$ with radius 1; and from this circle we can construct a square of area π. Each side of the square has length $\sqrt{\pi}$, so the point $(\sqrt{\pi}, 0)$ is constructible.

Then from the last homework assignment (problem 2, part e), $\mathbb{Q}(\sqrt{\pi})$ has finite degree 2^m over $\mathbb{Q}$. Then $\pi = \sqrt{\pi} \cdot \sqrt{\pi} \in \mathbb{Q}(\sqrt{\pi})$, so again from the last homework assignment (problem 1, part c), π is algebraic over $\mathbb{Q}$—a contradiction. Thus our original assumption was false, and we cannot square the circle by ruler and compass.

Problem 2.

(a) $K[X]$ is a principal ideal domain, so if some ideal I contained (p) then it must be generated by some polynomial q. Thus $q \mid p$ so (since p is irreducible) either $q = k$ or $q = kp$ for some constant $k \in K$. But $(k) = K[X]$ and $(kp) = (p)$, so (p) is a maximal ideal.

Let $L = K[x]/(p)$; since (p) is a maximal ideal, L is a field. Each element in L is of the form $q+(p)$ for $q \in K[X]$, where $q_1+(p) = q_2+(p)$ when $p \mid (q_1 - q_2)$. Let $\overline{q}$ denote $q + (p)$.

Then L contains K as a subfield (in the form of the elements $\overline{k}$ for each $k \in K$). And if $p = \sum_{i=0}^n a_i X^i$, then $p(\overline{X}) = \sum_{i=0}^n a_i \overline{X}^i = \sum_{i=0}^n a_i \overline{X^i} = \sum_{i=0}^n \overline{a_i X^i} = \overline{\sum_{i=0}^n a_i X^i} = \overline{p} = \overline{0}$. Thus writing $\alpha = \overline{X}$, we have $p(\alpha) = 0$. And L consists exactly of elements of the form $\sum_{i=0}^n a_i \alpha^i \in K[\alpha]$, so $L = K[\alpha]$.

(b) From our previous homework we know that $L_1 = \{q(\alpha_1) \mid q \in K[X]\}$ and $L_2 = \{q(\alpha_2) \mid q \in K[X]\}$.

Now suppose we have such an isomorphism ϕ. Given any $q \in K[X]$, write $q = \sum_{i=0}^n a_i X^i$ for $a_0, a_1 \ldots, a_n \in K$. Then

$$\begin{aligned}\phi(q(\alpha_1)) = \phi\left(\sum_{i=0}^n a_i \alpha_1^i\right) &= \sum_{i=0}^n a_i \phi(\alpha_1)^i \\ = \sum_{i=0}^n a_i \alpha_2^i &= q(\alpha_2).\end{aligned}$$

Because every element of L_1 can be written in the form $q(\alpha_1)$, it follows that such an isomorphism, if it exists, is unique.

Define ϕ by $\phi(q(\alpha_1)) = q(\alpha_2)$ for all polynomials $q \in K[X]$. This is well-defined and injective since for $q_1, q_2 \in K[X]$,

$$\begin{aligned}&q_1(\alpha_1) = q_2(\alpha_1) \text{ evaluated in } K[\alpha_1] \\ &\Longrightarrow (q_1 - q_2)(\alpha_1) = 0 \text{ evaluated in } K[\alpha_1] \\ &\Longrightarrow p \mid q_1 - q_2 \text{ in } K[X] \\ &\Longrightarrow (q_1 - q_2)(\alpha_2) = 0 \text{ evaluated in } K[\alpha_2] \\ &\Longrightarrow q_1(\alpha_2) = q_2(\alpha_2) \text{ evaluated in } K[\alpha_2].\end{aligned}$$

It is also surjective because every element of L_2 can be written in the form $q(\alpha_2)$. From Problem 1, the maps $q \mapsto q(\alpha_1)$ and $q \mapsto q(\alpha_2)$ are ring homomorphisms; hence,

$$\begin{aligned}&\phi\left(q_1(\alpha_1)q_2(\alpha_1)\right) = \phi\left((q_1 \cdot q_2)(\alpha_1)\right) = (q_1 \cdot q_2)(\alpha_2) \\ &\quad = q_1(\alpha_2)q_2(\alpha_2) = \phi(q_1(\alpha_1))\phi(q_2(\alpha_1)).\end{aligned}$$

Similarly, ϕ preserves addition (and the unit). It follows that ϕ is a field isomorphism, as desired.

(c) Observe that for a field F, if $X - \alpha \mid p$ for some $\alpha \in F$, $p \in F[X]$ then we can write $p = (X - \alpha)q$ for some polynomial $q \in F[X]$. This follows simply from the Euclidean algorithm because we can write $p = (X-\alpha)q + r$ for some polynomials $q, r \in F[X]$ with r a constant; and since $r(\alpha) = p(\alpha) - (X-\alpha)(\alpha)\cdot q(\alpha) = 0$, we must have $r = 0$.

We now prove a slightly more general claim than the one stated in the problem: given *any* nonconstant polynomial $p \in K[X]$, there exists an extension field L of K such that p splits into a product of linear factors in $L[X]$, and L is generated over K by the roots of p. (We'll call this a "pseudo-splitting field" since p doesn't have to be irreducible.)

We prove the claim by induction on the degree of p. When p is linear the claim is trivial (just take $L = K$).

So now assume that the claim is true for all polynomials with degree less than p. If p already splits into a product of linear factors in $K[X]$, we are done (just take $L = K$). Otherwise some irreducible p' of degree at least 2 divides p. Then from part (a), there exists an extension field L_1 of K and an element $\alpha_1 \in L_1$ such that $p'(\alpha_1) = 0$ and $L_1 = K[\alpha_1]$. Thus we can write $p = (X-\alpha_1)q$ for some polynomial $q \in L_1[X]$. If q is constant, we are done. Otherwise, by the induction hypothesis there is an extension field L_2 of L_1 such that q splits into a product of linear factors $(X-\alpha_2)(X-\alpha_3)\cdots(X-\alpha_n)$ in $L_2[X]$ and such that $L_2 = L_1[\alpha_2, \alpha_3, \ldots, \alpha_n]$. But then in $L_2[X]$, p splits into a product of linear factors $(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$; and $L_2 = L_1[\alpha_2, \alpha_3, \ldots, \alpha_n] = K[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is generated over K by the roots of p in $L_1[X]$. Thus there does exist a pseudo-splitting field of p; and this completes the inductive step, and the proof of the claim.

(d) Again we prove a slightly more general claim: given any polynomial $p \in K[X]$, there exists a *unique* pseudo-splitting field up to isomorphism over K. We prove the claim by induction on $\deg(p)$; when $\deg(p) = 1$, the claim is trivial.

Suppose we have two pseudo-splitting fields L_1 and L_2 of p. If p already splits into linear factors, then clearly we must have $L_1 = L_2 = K$ so we are done. Otherwise, let q be an irreducible nonlinear factor of p in $K[X]$. Since q can be written as a product of linear factors in $L_1[X]$, when viewed as a polynomial in $L_1[X]$ it has some root $r \in L_1$; then when viewed as a polynomial in $(K[r])[X]$ it has this root r. Similarly, there is some $s \in L_2$ such that when viewed as a polynomial in $(K[s])[X]$, q has s as a root.

Then from part (b), there exists an isomorphism ϕ over K of fields $K[r] \xrightarrow{\sim} K[s]$ mapping r to s. Now write $p \in (K[r])[X]$ as $(X-r)q_1$ for some $q_1 \in (K[r])[X]$. Writing $q_1 = \sum_{i=0}^{n} \gamma_i X^i$, let $q_2 = \sum_{i=0}^{n} \phi(\gamma_i) X^i$

for $i = 0, 1, \ldots, n$. The coefficients of $(X - r)q_1 \in (K[r])[X]$ are polynomials in r and the γ_i, and the coefficients of $(X - s)q_2 \in (K[s])[X]$ are analogous polynomials in $s = \phi(r)$ and the $\phi(\gamma_i)$. Because ϕ preserves multiplication and addition, it follows that it maps each coefficient of $p = (X - r)q_1$ to the corresponding coefficient in $(X - s)q_2$. But each such coefficient of p is in K and hence fixed by ϕ, implying that $(X - s)q_2 = p$ in $(K[s])[X]$.

Observe that L_1 is a pseudo-splitting field over $K[r]$ of q_1; and clearly L_1 is isomorphic over K to *some* splitting field L_2' over $K[s]$ of q_2. But L_2 is also a pseudo-splitting field over $K[s]$ of q_2; and since $\deg(q_2) < \deg(p)$, by the induction hypothesis L_2 is *also* isomorphic over K to L_2'. Therefore L_1 and L_2 are isomorphic over K, as desired.

Note: The "clearly" in the last paragraph is a bit of a cop-out. Recall that one field K_1 can be considered as a subfield of another field K_2 in two ways – either by actually sitting inside K_2, or by being isomorphic to another field that sits inside K_2. If we use the first interpretation, we can concoct the field $L_2' = (L_1 \setminus K[r]) \cup K[s]$ and twist this set around a bit to define addition and multiplication correctly. If we use the second interpretation, we can let $L_2' = L_1$ because $K[r] \subset L_1$ is isomorphic to $K[s]$. (Personally, the second interpretation seems more natural: in general, isomorphism seems more useful and natural than strict equality. It's somewhat strange to talk about *the* group of permutations on a set of three elements, for example: this group is in some sense different given different three-element sets, but all such groups are isomorphic. See the solutions to Assignment 12 to see how the result "pseudo-splitting fields are unique" might be applied using isomorphic, not necessarily identical, base fields.)

Problem 3.

Given a projection operator $p : V \to V$, we know that $v \in \operatorname{Ker} p$ if and only if $p(v) = 0$. Also observe, though, that $v \in \operatorname{Im} p$ if and only if $p(v) = v$: if $p(v) = v$ then v is in the image; and if $v = p(v')$ then $p(v) = p(p(v')) = p(v') = v$.

(a) Suppose p is a projection operator; clearly $1_V - p$ is a linear transformation. Now given $v \in V$, note that $(1_V - p)(v) = v - p(v)$. Then $(1_V - p)^2(v) = (1_V - 2p + p^2)(v) = ((1_V - p) + (p^2 - p))(v)$. But $p^2 - p = 0$ since p is a projection operator. Thus,

$$(1_V - p)^2(v) = (1_V - p)(v)$$

for all $v \in V$, implying that $1_V - p$ is indeed a projection operator.

(b) Suppose that $k_1 + i_1 = k_2 + i_2$ for $k_1, k_2 \in \operatorname{Ker} p$ and $i_1, i_2 \in \operatorname{Im} p$. Then

$$p(k_1 + i_1) = p(k_2 + i_2) \Longrightarrow p(k_1) + p(i_1) = p(k_2) + p(i_2) \Longrightarrow i_1 = i_2.$$

Because $k_1 + i_1 = k_2 + i_2$, we also have $k_1 = k_2$. Hence, each element in V can be written in such a form in at most one way.

But given $v \in V$, write $i = p(v)$ and $k = v - i$. Then

$$p(k) = p(v) - p(i) = i - i = 0$$

so $k \in \operatorname{Ker} p$; and by construction $i \in \operatorname{Im} p$ and $v = k + i$. Thus every element in V can be written in the form $k + i$ (for $k \in \operatorname{Ker} p$, $i \in Ker i$) in *exactly* one way, so indeed $V = \operatorname{Ker} p \oplus \operatorname{Im} p$.

(c) If p is such a projection operator, then from our initial observations $p(w_1) = 0$ for all $w_1 \in W_1$; and $p(w_2) = w_2$ for all $w_2 \in W_2$. Since any v can be written uniquely in the form $w_1 + w_2$ for $w_1 \in W_1, w_2 \in W_2$ we must have $p(v) = p(w_1) + p(w_2) = w_2$. Thus if there is such a projection operator, it is unique.

Now we show that the map described above — $p(v)$ is the unique value $w_2 \in W_2$ such that $v - w_2 \in W_1$ — is indeed a projection operator. For $w_1, w_1' \in W_1$ and $w_2, w_2' \in W_2$, and any $\kappa \in K$, we have $p(\kappa(w_1 + w_2)) = p(\kappa w_1 + \kappa w_2) = \kappa w_2 = \kappa p(w_1 + w_2)$ and $p(w_1 + w_2 + w_1' + w_2') = w_2 + w_2' = p(w_1 + w_2) + p(w_1' + w_2')$, so p is a linear transformation. And because $p(p(w_1 + w_2)) = p(w_1 + w_2) = w_2$, it is a projection operator.

(d) Because $V = W_1 \oplus W_2$ and because $p \circ T$, $T \circ p$ are linear, p and T commute iff for $i = 1, 2$,

$$(p \circ T)|_{W_i} = (T \circ p)|_{W_i}. \qquad (\dagger)$$

For $i = 1$, because $p|_{W_1} = 0$, the right hand side of (†) is zero. Hence (†) is true for $i = 1$ iff the left hand side is zero — i.e., iff $p(T(W_1)) = \{0\}$, or equivalently iff $T(W_1) \subset \operatorname{Ker} p = W_1$.

For $i = 2$, because $p|_{W_2} = 1_{W_2}$, the right hand side of (†) is $T|_{W_2}$. Hence (†) is true for $i = 2$ iff the left hand side is $T|_{W_2}$ — i.e., iff p fixes each element of $T(W_2)$, or equivalently iff $T(W_2) \subset W_2$.

Therefore, p and T commute iff (†) is true, and this holds iff W_1 and W_2 are T-invariant.