Lüroth's Theorem, and some related results, developed as a series of exercises

A *simple transcendental extension* of a field k means an extension of the form $k(t)$ where t is transcendental over k; in other words, an extension isomorphic to the field of rational functions in one indeterminate over k. Throughout this set of exercises, $k(t)$ will denote such a field.

We shall prove that every subextension of $k(t)$, other than k itself, is also a simple transcendental extension of k. We shall need to consider algebraic relations satisfied by elements of $k(t)$ over subfields, hence we shall work with the polynomial ring $k(t)[x]$. In calculating with elements of this ring we shall make use of the subring $k[t, x]$, which is a polynomial ring over k in two indeterminates.

(1) Show that every nonzero element $f \in k(t)[x]$ can be written uniquely $f = P(t,x)/Q(t)$ where $P(t,x) \in k[t, x]$, $Q(t) \in k[t]$, P and Q are relatively prime in the unique factorization domain $k[t, x]$, and Q is monic as a polynomial in t.

From now on, whenever we write an element $f \in k(t)[x]$ as $P(t,x)/Q(t)$, we shall understand P and Q to have the above properties. In this situation, let us define the *height* of f to be the nonnegative integer $\mathrm{ht}(f) = \max(\deg_t(P(t,x)), \deg_t(Q(t)))$, where $\deg_t$ means ''degree as a polynomial in t''.

In particular, if $u \in k(t)$ and we write $u = P(t)/Q(t)$, then the above assumptions on P and Q, and the above definition of the height $\mathrm{ht}(u)$, will be understood to apply.

(2) Suppose $f = P(t,x)/Q(t)$ is *monic* as a polynomial in x over $k(t)$. Show that $\mathrm{ht}(f) = \deg_t(P(t,x))$, and that $P(t,x)$ is not divisible by any nonunit element of $k[t]$.

(3) Deduce that if $f, g \in k(t)[x] - \{0\}$ are both monic as polynomials in x, then $\mathrm{ht}(fg) = \mathrm{ht}(f) + \mathrm{ht}(g)$.

(4) If u is any element of $k(t)$ not in k, show that there is an element u', of the same height as u, such that $k(u') = k(u)$, and with the properties that when u' is written $P'(t)/Q'(t)$ we have $\deg_t(P') > \deg_t(Q')$, and that P' (as well as Q') is monic.

(You will find that u' can be taken to be of the form αu or $\alpha/(u-\beta)$, where $\alpha, \beta \in k$.)

The next observation shows that t, though transcendental over k, is algebraic over any nontrivial intermediate field.

(5) Given any $u = P(t)/Q(t) \in k(t) - k$, verify that t is a root of the polynomial $P(x) - uQ(x) \in k(u)[x]$. Show further that if $\deg_t(P) > \deg_t(Q)$, and P is monic, then the above polynomial is monic.

Now suppose L is any intermediate field: $k \subset L \subseteq k(t)$. Let $u = P(t)/Q(t)$ be an element of $L - k$ chosen to minimize $n = \mathrm{ht}(u)$, and, using (4), also taken so that $\deg_t(P) > \deg_t(Q)$ and P is monic. These conditions will be assumed in the next three steps.

(6) Show that every polynomial $f \in L[x]$ has height either 0 or $\geq n$, and that $P(x) - uQ(x)$ has height exactly n; deduce from (3) that $P(x) - uQ(x)$ is either irreducible in $L[x]$, or divisible by a nonunit element of $k[x]$.

(7) Show that if $P(x) - uQ(x)$ is divisible in $L[x]$ by an element of $k[x]$, then this element must divide both $P(x)$ and $Q(x)$. Deduce that this element must be a unit. (Suggestion for the first assertion: extend $\{1, u\}$ to a basis of L over k. You might prove that assertion in the general context of divisibility of a polynomial over any field L by a polynomial over a subfield k. The second assertion depends on our assumptions on P and Q, specific to our present situation.)

(8) Conclude that $P(x) - uQ(x)$ is the minimal polynomial of t over L. Deduce that $P(x) - uQ(x)$ is also the minimal polynomial of t over $k(u) \subseteq L$, and from this that $L = k(u)$.

(9) Deduce:

Lüroth's Theorem. *If $k(t)$ is a simple transcendental extension of a field k, and $k \subset L \subseteq k(t)$, then L is also a simple transcendental extension of k, and is generated over k by any element $u \in L$ of minimal positive height. Moreover,* $[k(t) : L] = \mathrm{ht}(u)$.

To tie things up, we would like to be able to conclude that for every element $u \in k(t) - k$, $[k(t){:}k(u)] = \mathrm{ht}(u)$. Unfortunately, we have only proved (8) for elements u having minimal height in an intermediate field L, and nothing we have proved excludes the possibility that if we start with a random element u, $k(u) - k$ might contain an element of smaller height than u. The only way I see to get the desired result is to give a second proof of the irreducibility of $P(x) - uQ(x)$, with the hypothesis of minimal height replaced by the hypothesis $L = k(u)$.

(10) Show for arbitrary $u = P(t) / Q(t) \in k(t) - k$ that $P(x) - uQ(x)$ is irreducible in $k(u)[x]$. (Hint: Apply Gauss's Lemma to $k[u]$.)

(11) Deduce that in the above situation, $[k(t){:}k(u)] = \mathrm{ht}(u)$, and conclude that u *is* of minimal height in $k(u) - k$.

(12) Deduce the following result, including the ''that is'' clause. (This is essentially Exercise V.2.6(d) of Hungerford; cf. Exercise IV.10 of Lang),

Corollary. *The simple generators of $k(t)$ as an extension field of k are precisely the elements of height* 1*, that is, the elements of the form $(at + b) / (ct + d)$ with* $ad - bc \neq 0$*. Hence every automorphism of $k(t)$ over k takes t to an element of this form.*

Lüroth's Theorem is analogous to the result that a nontrivial subgroup of the free abelian group $\mathbf{Z}$ of rank 1 is free of rank 1, is generated by any element of minimal absolute value, and has index in $\mathbf{Z}$ equal to this absolute value. However, analogous results do not hold in all situations:

(13) Show that the subalgebra $k[x^2, x^3] \subseteq k[x]$ is not a polynomial ring over k. (Suggestion: show it is not a unique factorization domain.)

If one looks at subfields of fields of rational functions in more than one indeterminate, the analog of Lüroth's Theorem fails – these need not, in general, be isomorphic to rational function fields. However, to give counterexamples, and to develop the partial positive results that do hold, we would need the theory of transcendence degree, and the concept of separability for transcendental extensions (Hungerford, Chapter VI; Lang, Chapter VIII).