HOMEWORK #2
SOLUTIONS TO SELECTED PROBLEMS

Problem 2.1. One has $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$. All the binomial coefficients $\binom{p}{i}$ are divisible by p for $0 < i < p$, as they have p factor in the nominator and no p factor in the denominator.

Problem 2.2. The proof is by induction on n, the case $n = 1$ being trivial.

Denote by K_i the subfield $K(\alpha_1, \ldots, \alpha_i)$, then obviously $K_1 \subset K_2 \ldots K_{n-1} \subset K_n$. By definition, $F_n = F_{n-1}(\alpha_n)$ is the minimal subfield of L containing F_{n-1} and α_n. But by the induction hypothesis, $F_{n-1} = K_{n-1}$. Now K_n is a field containing K_{n-1} and α_n, so by minimality $K_n \supset F_n$.

On the other hand, K_n is the minimal field containing K and $\alpha_1, \ldots, \alpha_n$. But $F_n = F_{n-1}(\alpha_n) = K_{n-1}(\alpha_n)$ is a subfield of L containing $\alpha_1, \ldots, \alpha_n$, so that $F_n \supset K_n$.

Problem 2.3. We construct an isomorphism $L_n \simeq K(t_1, \ldots, t_n)$ by induction on n. For $n = 1$ this is clear. For $n \geq 0$, it is enough to construct an isomorphism $K(t_1, \ldots, t_n)(t) \simeq K(t_1, \ldots, t_{n+1})$, since

$$L_{n+1} = L_n(t) \simeq K(t_1, \ldots, t_n)(t) \simeq K(t_1, \ldots, K_{n+1})$$

where the first isomorphism follows by the induction hypothesis (any isomorphism $F \simeq E$ can be extended to the fields of rational functions $F(t) \simeq E(t)$ by the action on coefficients).

We construct the isomorphism $K(t_1, \ldots, t_n)(t) \simeq K(t_1, \ldots, t_{n+1})$ in steps. First, we define a monomorphism of rings $K(t_1, \ldots, t_n)[t] \to K(t_1, \ldots, t_{n+1})$. Then we use the following lemma

Lemma. *Let A be a commutative integral domain and $f : A \to L$ a monomorphism of rings into a field L. Consider the embedding $i : A \to K(A)$ into the fraction field of A. Then there exists a unique extension of f to a monomorphism of fields, $\tilde{f} : K(A) \to L$, such that $\tilde{f} \circ i = f$ (on A).*

to define $K(t_1, \ldots, t_n)(t) \to K(t_1, \ldots, t_{n+1})$. Finally, we show that this one-to-one map is also surjective (onto).

Step 1. An element of $K(t_1, \ldots, t_n)[t]$ has the form $\sum_i (p_i/q_i) t^i$ where $p_i, q_i \in K[t_1, \ldots, t_n]$ are polynomials in n variables. So we map this element to the element

$$\sum_i \frac{p_i(t_1, \ldots, t_n) t_{n+1}^i}{q_i(t_1, \ldots, t_n)} = \frac{\sum_i (\prod_{j \neq i} q_j(t_1, \ldots, t_n)) p_i(t_1, \ldots, t_n) t_{n+1}^i}{\prod_i q_i(t_1, \ldots, t_n)}$$

in $K(t_1, \ldots, t_{n+1})$

One has to check that this is well defined by verifying that by taking another representative of the same element in $K(t_1, \ldots, t_n)[t]$ we land in the same element of $K(t_1, \ldots, t_{n+1})$.

It is clear that the map defined is a homomorphism of rings. It is also one-to-one since any non-zero polynomial over $K(t_1, \dots, t_n)$ gets mapped to a non-zero element of $K(t_1, \dots, t_{n+1})$ (look at the nominator and verify that it is non-zero if at least one of the p_i is non-zero).

Step 2. We prove the lemma. The *uniqueness* of $\tilde{f}$ follows from the fact that for any $a, b \neq 0$ in A we must have

$$\tilde{f}(a/b) = \tilde{f}(a/1)\tilde{f}(1/b) = \tilde{f}(i(a))/\tilde{f}(i(b)) = f(a)/f(b)$$

So we *define* $\tilde{f}(a/b) = f(a)/f(b)$. This is well defined since $f(b) \neq 0$ for $b \neq 0$ (f is a monomorphism), and if $c/d = a/b$ then $ad = bc$ hence $f(a)f(d) = f(ad) = f(bc) = f(b)f(c)$ so that $f(a)/f(b) = f(c)/f(d)$ is independent of the representation of element in $K(A)$. It is easy to see that $\tilde{f} : K(A) \to L$ is a monomorphism.

Step 3. By step 2 we get $K(t_1, \dots, t_n)(t) \to K(t_1, \dots, t_{n+1})$. To prove this map is onto, take an element in $K(t_1, \dots, t_{n+1})$, write it as a ratio P/Q of polynomials, and write P, Q as polynomials in t_{n+1} with coefficients in $K[t_1, \dots, t_n]$, i.e. $P = \sum_i p_i(t_1, \dots, t_n)t_{n+1}^i$, $Q = \sum_i q_i t_{n+1}^i$. Verify that the image of the element

$$\frac{\sum_i \frac{p_i}{1}(t_1, \dots, t_n)t^i}{\sum_i \frac{q_i}{1}(t_1, \dots, t_n)t^i} \in K(t_1, \dots, t_n)(t)$$

is P/Q.

Problem 2.4. (a) Since $q(t) = t^7 - t^4 + t^3 - 1 = (t^3 - 1)(t^4 + 1)$, the greatest common divisor of $q(t)$ and $t^3 - 1$ is $t^3 - 1$.

To prove (b) and (c), note that $[K[x]/(f) : K] = \deg f$ for any irreducible polynomial $f \in K[x]$ (problem 1.5). The polynomials in (b), (c) are irreducible since they are of degrees 2, 3 and have no roots in the base field (see lemma in the solution to problem 1.4).

Problem 2.5. We prove that for *any* polynomial $f \in K[t]$ of positive degree n, there is an extension L of K such that f splits in L and $[L : K] \leq n!$.

The proof is by induction on $n = \deg f$. For $n = 1$, f is linear hence has exactly one root in K, so we take $L = K$.

Now let $f \in K[t]$ be of degree n. We treat two cases:

1. f is reducible. In this case, write $f = gh$. Write $m = \deg g < n$ and $n - m = \deg h < n$. By the induction hypothesis for g and K, there exists an extension $K' \supset K$ such that g splits in K' and $[K' : K] \leq m!$. Now, $h \in K[t] \subset K'[t]$, so by the induction hypothesis for h and K', there exists an extension $L \supset K'$ such that h splits in L and $[L : K'] \leq (n-m)!$. It is easy to see that f splits in L and $[L : K] = [L : K'][K' : K] \leq m!(n-m)! < n!$.

2. f is irreducible. Take $K' = K[t]/(f)$. Then $K' \supset K$ is an extension of degree n which has a root of f (namely, the image of t), denote it α. Then in $K'[t]$ there is a factorization $f(t) = (t - \alpha)g(t)$ with $g \in K'[t]$ and $\deg g = n - 1$. By the induction hypothesis for g and K', there is an extension $L \supset K'$ such that g splits in L and $[L : K'] \leq (n-1)!$. Then f splits in L and $[L : K] = [L : K'][K' : K] \leq (n-1)!n = n!$.