QUESTION: (HD 1302) Let L/K be a fields extension such that L is algebraic over K. Does there exists a positive integer m such that every irreducible element of K[X] (polynomial ring over K) has factorization

of finite length less than m in L[X] ? If the response is "no", what are the couple (K,L) on which the response is "yes".

ANSWER: Let us say that L/K has a bound b if every irreducible polynomial of $K[X]$ has length less than b in $L[X]$.

Let A be the field of all algebraic numbers. Then A/Q is algebraic and every polynomial in $Q[X]$ is a product of linear polynomials in $A[X]$. Since $Q[X]$ has irreducible polynomials of every degree (such as $X^n - 2$) we conclude that A/Q does not have a bound m. Another example of an algebraic extension L/K without a bound can be $K = GF(p^n)$ and $L = GF(p^\infty) = \cup GF(p^{n!})$ the algebraic closure of $GF(p)$ and hence of $GF(p^n)$. Here too, as $GF(p^n)$ has irreducible polynomials of every degree which split into linear factors in $GF(p^\infty)$ and so there is no bound for L/K. (Let $q = p^m$ and let $N_q(n)$ be the number of monic irreducible polynomials of degree n in $GF(q)[X]$, then $N_q(n) = \frac{1}{n}\sum \mu(d)q^{\frac{n}{d}}$, where $\mu(x)$ is the Mobius function. The formula shows that $N_q(n)$ is positive for all n. This is Theorem 7.13 in the link given below.

http://www-groups.mcs.st-and.ac.uk/~neunhoef/Teaching/ff/ffchap3.pdf

However you cannot always take L/K where L is the algebraic closure of K and shout "here's the counter-example!" The following statement may cover some of the cases where L/K may be bounded by some b, and L is the algebraic closure of K.

Observation A: Let L/K be an algebraic extention of fields such that there is no irreducible polynomial in $K[X]$ of degree greater than m, where $m > 1$.Then L/K has a bound $m + 1$.

Illustration: Let $g(X)$ be an irreducible polynomial in $K[X]$. Then $\deg(g(X)) \leq m$, and so length$(g(X)) \leq m$ in $L[X]$ and so less than $m + 1$.

The above "Observation" is not quite an empty one. Consider the case of C/R where C is the field of complex numbers and R the field of real numbers. We know that every polynomial of degree greater than 2 is reducible in $R[X]$ and so the length of each irreducible polynomial of $R[X]$ is ≤ 2 in $C[X]$ which means that 3 is a bound of C/R.

The above Observation also applies to the case where K is a real closed field and L the algebraic closure of K.

These are just preliminary observations. I hope they are of help. If my health holds I might look into it some more.

1-26-2013

Remark 1. I wrote a preliminary version of the above answer and sent it around for a check. Two e-mails came, one from Franz Halter-Koch and the other from Tiberiu Dumitrescu. Both of them said that L/K is bounded when $[L : K] < \infty$. Tiberiu gave the following proof.

Observation B. Let L/K be an algebraic extention of fields such that $[L : K] = n$. Then L/K has a bound $n + 1$.

Proof. Let $f(X) \in K[X]$ be an irreducible polynomial of degree $p \geq n + 1$. Assume that f splits into at least $n + 1$ irreducible factors: $f = h_1 h_2 \ldots h_r$ in $L[X]$. One of these irreducible factors say h_1 is such that $\partial h_1 = \min\{\partial h_i\}_{i=1}^{r}$. Then $r\partial h_1 \leq \sum \partial h_i = p$ here ∂h_i denotes the degree of h_i. So $\partial h_1 \leq \frac{p}{r} \leq \frac{p}{n+1}$ as $r \geq n + 1$. Now let z be a root of h_1 in some extension of L. Then $h_1(z) = 0$ and hence $f(z) = 0$. Since f is irreducible f is the irreducible polynomial of z over K. Thus $[K(z) : K] = \partial f = p$. On the other hand $[L(z) : L] = \partial h_1 \leq \frac{p}{n+1}$.

Next note that $[L(z) : K] \geq [K(z) : K] = p$. So $[L(z) : K] \geq p$.

On the other hand $[L(z) : K] = [L(z) : L][L : K] = \partial h_1 n \leq \frac{p}{n+1} n < p$, a contradiction.

In a later e-mail, Tiberiu provided an alternatione proof of Observation B. As the proof also gives a handle on the multiplicities of irreducible divisors, I include it below.

Alternative proof of Observation B. Theorem 21 at page 285 of Zariski-Samuel, Commutative Algebra vol I, first edition says: Let A be a Dedekind domain with qoutient field K, L a finite field extension of K, B the integral closure of A in L. Let P be a maximal ideal of A and let $PB = (Q_1)^{e_1}(Q_2)^{e_2}\ldots(Q_g)^{(e_g)}$ be the prime ideal decomposition of PB. Then $e_1 f_1 + \ldots + e_g f_g \leq n$ where $n = [L : K]$ and $f_i = [B/Q_i : A/P]$. Now let L/K be a finite field extension of degree n. We just apply the theorem for $A = K[X]$ and $B = L[X]$, noting that $K(X) \subset L(X)$ is again a finite field extension of degree n.

Remark 2. At one point it was suggested that if $F = Q(\{2^{\frac{1}{p^n}} : n \in N\})$ then F/Q is bounded. But the following consideration shows that for each n the polynomial $X^{p^n} - 2$ has more than n factors, and hence is of length more than n.

The field $F = Q(\{2^{\frac{1}{p^n}} : n \in N\})$ is an ascending union of fields $Q(2^{\frac{1}{p^n}})$. The degree of each of these fields is p^n. Indeed $Q(2^{\frac{1}{p^n}}) \subseteq Q(2^{\frac{1}{p^{n+1}}})$ and $[Q(2^{\frac{1}{p^{n+1}}}) : Q(2^{\frac{1}{p^n}})] = p$. So there are no fields lying properly between any two consecutive constituent fields. Thus for each $\alpha \in Q(2^{\frac{1}{p^{n+1}}})\backslash Q(2^{\frac{1}{p^n}})$, $Q(2^{\frac{1}{p^n}})(\alpha) = Q(2^{\frac{1}{p^{n+1}}})$ and so α satisfies a polynomial of degree p over $Q(2^{\frac{1}{p^n}})$. Next if $\alpha \in Q(2^{\frac{1}{p^{n+1}}})\backslash Q(2^{\frac{1}{p^n}})$ satisfies an irreducible polynomial $f(X)$ over Q then the degree of f is p^{n+1}. Thus if $\alpha \in Q(2^{\frac{1}{p^r}})$ and $\beta \in Q(2^{\frac{1}{p^{r+s}}})\backslash Q(2^{\frac{1}{p^r}})$ then α and β cannot be the roots of the same irreducible polynomial. This leaves two or more possible roots of an irreducible polynomial in $Q(2^{\frac{1}{p^{n+1}}})\backslash Q(2^{\frac{1}{p^n}})$ for some n. There is of course the occurrence of roots, in an extension field involving ζ, where ζ is the pth root of unity, satisfying $f(X)$ that need to be ruled out, and of course roots in other extension fields. This led me to look for a counter-example.

My example is an irreducible polynomial of the form $X^{p^n} - 2$ over $Q[X]$.

This factorizes as

$X^{p^n} - 2 = (X^{(p^{n-1})})^p - 2 = (X^{p^{n-1}} - 2^{\frac{1}{p}})((X^{p^{n-1}})^{p-1} + 2^{\frac{1}{p}}(X^{p^{n-1}})^{p-2} + 2^{\frac{2}{p}}(X^{p^{n-1}})^{p-3} + \ldots + 2^{\frac{p-1}{p}}) =$ $(X^{p^{n-1}} - 2^{\frac{1}{p}})f_1(X)$ in $Q(2^{\frac{1}{p}})[X]$ where $f_1(X)$ is a prime over $F[X]$ or a product of primes. Next using the same trick $(X^{p^{n-1}} - 2^{\frac{1}{p}})$ factorizes in $Q(2^{\frac{1}{p^2}})[X]$ in the same manner since $X^{p^{n-1}} = (X^{p^{n-2}})^p$ and $\sqrt[p]{2^{\frac{1}{p}}} = 2^{\frac{1}{p^2}}$. So $(X^{p^{n-1}} - 2^{\frac{1}{p}}) = (X^{p^{n-2}} - 2^{\frac{1}{p^2}})f_2(X)$ giving $X^{p^n} - 2 = (X^{p^{n-2}} - 2^{\frac{1}{p^2}})f_2(X)f_1(X)$ in $Q(2^{\frac{1}{p^2}})[X]$ and hence in $F[X]$. Continuing thus we have

$X^{p^n} - 2 = (X - 2^{\frac{1}{p^n}})f_n(X)f_{n-1}(X)\ldots f_2(X)f_1(X)$ more than n factors in $Q(2^{\frac{1}{p^n}})[X]$ and hence in $F[X]$ for every $n \in N$. Thus F/Q is unbounded.

Dated: 2-1-2013