Supernatural numbers:

A supernatural number $\omega$ is a formal product $\omega = \prod p^{n_p}$, where $p$ runs over all (rational) prime numbers, and the values $n_p$ are each either natural numbers or the symbol $\infty$. Clearly, every natural number can be viewed as a supernatural number. If $\omega' = \prod p^{n_p'}$ and $\omega'' = \prod p^{n_p''}$ are such numbers, we define their product by $\omega' \omega'' = \prod p^{n_p}$, where $n_p = n_p' + n_p''$ with the rule $a + \infty = \infty$. Remark that this multiplication extends the multiplication of natural numbers. Further we say that $\omega'$ divides $\omega''$, written $\omega'/|\omega''$, if $n_p' \leq n_p''$ for all $p$. Remark that this notion of divisibility extends the one defined for natural numbers.

The supernatural numbers are used to define the “degree” of arbitrary algebraic field extension: Let $L/K$ be a field extension. For every finite sub-extension $M/K$ we let $n_p,M$ be the exponent of $p$ in $[M : K]$; and set $n_p := \sup_{M} (n_{p,M})$. We denote $[L : K] = \prod p^{n_p}$, and call it the degree of $L/K$. They are also used to define the “order” and/or the index of profinite groups as follows: Let $G$ be a profinite group, and $H \subseteq G$ a closed subgroup. For every open normal subgroup $\Delta$ of $G$, let $\overline{H} \subset \overline{G}$ be the image of $H$ in $\overline{G} := G/H$; and let $n_p,\Delta$ be the exponent of $p$ in $([\overline{G} : \overline{H}]$. Finally we set $n_p = \sup_{\Delta}(n_{p,\Delta})$, and denote $(G : H) = \prod p^{n_p}$, and call it the index of $H$ in $G$. If $H = \{1\}$ is the trivial group, then $|G| := (G : 1)$ is called the order of $G$.

1) In the above context/notations prove the following:

a) If $H \subseteq G$ is a closed subgroup, then $[H]$ divides $[G]$, and $[G] = (G : H)[H]$. Further, $H$ is open in $G \iff (G : H)$ is a natural number.

b) If $M/K$ is a sub-extension of $L/K$, then $[L : K] = [L : M][M : K]$. Further, $L/K$ is finite $\iff [L : K]$ is a natural number.

c) Let $L/K$ be a Galois extension, $G = G(L/K)$ its Galois group, and $\text{gal} : F(L/K) \rightarrow G(L/K)$ the Galois correspondence. Show that for all $M \in F(L/K)$ one has: $[L : M] = |\text{gal}(M)|$, and that for all $H \subseteq G(L/K)$ one has: $[L : L^H] = (G : H)$.

Trace, Norm, Discriminants:

2) Let $L = \mathbb{k}[x]$ be a finite field extension of degree $n = [L : K]$. Let $P(X) = \text{Mip}_K(x)$, and $P'(X)$ be its formal derivative. Finally set $A := \{1, x, \ldots, x^{n-1}\}$ —this is a $K$-basis of $L$ (WHY?).

a) $\text{disc}(A) = \pm N_{L/K}(P'(x))$. What is the precise sign $\pm 1$ in this formula?

b) Supposing that $x$ is separable, compute the reciprocal basis $A^*$ of $A$.

3) Let $K = \mathbb{Q}$, and $L/K$ be a finite extension (thus $L$ is a number field), $n = [L : K]$.

a) Show that there exists a unique square free integer $d_L$ such that the discriminants of the several bases $A$ of $L$ over $K$ are of the form $\text{disc}(A) = d_L \cdot d_A^2$ for some rational number $d_A$.

b) For $L = \mathbb{Q}[x]$ with $x = \sqrt{2}$, $x = \sqrt{3}$, $x = \sqrt{5}$, and $A = \{1, x, \ldots, x^{n-1}\}$, find both $d_L$ and $d_A$.

c) Prove or disprove: If $L \neq \mathbb{Q}$, then $d_L \neq 1$.

d) Prove or disprove: For every $a \in \mathbb{Q}^\times$ there exists a basis $A$ such that $d_A^2 = a^2$.

4) Let $L/K$ be a finite field extension, $M/K$ a sub-extension. For $x \in L$, we set $y = \text{Tr}_{L/M}(x)$, $z = N_{L/M}(x)$. Prove or disprove the following:

a) If $x$ is a primitive element for $L/K$, then $y$ and/or $z$ are primitive elements of $M/K$.

b) There exists primitive elements $x$ for $L/K$ such that $y$ and/or $z$ are primitive elements of $M/K$.

Now suppose that $L/K$ and $M/K$ are Galois and finite. Recall that an element $u$ is called a normal generator, if its conjugates define a $K$-basis (of the Galois field extension in discussion).

c) If $x$ is a normal generator for $L/K$, then $y$ and/or $z$ are normal generators of $M/K$.

d) There exist normal generators $x$ of $L/K$, such that $y$ and/or $z$ are normal generators of $M/K$. 

Due: Monday, Nov 28, 2005

Grad Algebra (602) / Problem Set 9