MATH 250B: COMMUTATIVE ALGEBRA HOMEWORK #9

JOHN VOIGHT

Problem R1. Show that -1 is a square in \mathbb{Z}_5 .

Solution. Although one can prove this directly, it is worth noting the following general result:

Let $f(x) \in \mathbb{Z}[x]$, let p be a prime, and suppose that there exists $\alpha_1 \in \mathbb{Z}/p\mathbb{Z}$ such that $f(\alpha_1) \equiv 0 \pmod{p}$ and $f'(\alpha_1) \not\equiv 0 \pmod{p}$. Then there exists a unique root $\alpha \in \mathbb{Z}_p$ of f satisfying $\alpha \equiv \alpha_1 \pmod{p}$.

Since $\mathbb{Z}_p = \lim_{n \to \infty} \mathbb{Z}/p^n \mathbb{Z}$, giving a root α of f in \mathbb{Z}_p is equivalent to giving for each $n \ge 1$ a root $\alpha_n \in \mathbb{Z}/p^n \mathbb{Z}$ of f such that $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$: then $\lim_{n \to \infty} \alpha_n = \alpha$ is a root of f in \mathbb{Z}_p .

We prove the existence of α_n by induction. We are given $\alpha_1 \in \mathbb{Z}/p\mathbb{Z}$. Given α_n , we lift it to $\alpha_{n+1} = \alpha_n + tp^n \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ as follows: since

$$f(\alpha_{n+1}) = f(\alpha_n + tp^n) \equiv f(\alpha_n) + tp^n f'(\alpha_n) \pmod{p^{n+1}}$$

by Taylor expansion, and $f(\alpha_n) \equiv 0 \pmod{p^n}$, it is enough to solve

$$f'(\alpha_n)t \equiv -f(\alpha_n)/p^n \pmod{p}$$

for t which is possible (uniquely) because $f'(\alpha_n) \equiv f'(\alpha_1) \not\equiv 0 \pmod{p}$. In our case, we may take $\alpha_1 = 2$ since $f'(2) = 4 \pmod{5}$.

Problem R2. Let *E* be the set consisting of all nonnegative integers, together with an extra element ∞ . A supernatural number is a formal product $\prod_p p^{e_p}$ where the product runs over all primes *p* and where the exponents e_p are elements of *E*. If *m* is a supernatural number, let $m\hat{\mathbb{Z}}$ be the intersection of the groups $n\hat{\mathbb{Z}}$, taken over positive integers *n* that divide *m*.

Show that the set of closed subgroups of $\widehat{\mathbb{Z}}$ corresponds bijectively with the set of supernatural numbers under the map $m \mapsto m\widehat{\mathbb{Z}}$.

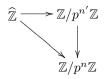
Solution. Let m be a supernatural number. We note that $m\widehat{\mathbb{Z}}$ is indeed a closed subgroup of $\widehat{\mathbb{Z}}$ since it is the intersection of the open (by definition) hence closed subgroups $n\widehat{\mathbb{Z}}$ for $n \in \mathbb{Z}$.

For each prime p and $n \in \mathbb{Z}_{>0}$, we have the projection map $\widehat{\mathbb{Z}} \to \mathbb{Z}/p^n\mathbb{Z}$. These maps are continuous (by definition) and are compatible in the sense that if $n' \ge n$,

Date: May 16, 2003.

R1–R4, VIII: 2–7.

the diagram



commutes. By the property of projective limits, we obtain a continuous map $\widehat{\mathbb{Z}} \to \lim_{n \to \infty} \mathbb{Z}/p^n \mathbb{Z} = \mathbb{Z}_p$. (In fact, the map $\widehat{\mathbb{Z}} \to \prod_p \mathbb{Z}_p$ is an isomorphism of topological rings if the product is given the product topology.)

From this we see that the map $m \mapsto m\widehat{\mathbb{Z}}$ is injective: if $m \neq m'$, then there exists a prime p such that $e_p \neq e'_p$ (where $m' = \prod_p p^{e'_p}$), hence the images of $m\widehat{\mathbb{Z}}$ and $m'\widehat{\mathbb{Z}}$ in \mathbb{Z}_p are different.

Let H be a closed subgroup of $\widehat{\mathbb{Z}}$. Since $\widehat{\mathbb{Z}}$ is compact (it is a closed subset of $\prod_m \mathbb{Z}/m\mathbb{Z}$ in the product topology and each factor is discrete), the image of H in \mathbb{Z}_p is compact; since \mathbb{Z}_p is Hausdorff (it is a subset of $\prod_n \mathbb{Z}/p^n\mathbb{Z}$, each factor again discrete), this image is closed. Let e_p be the largest element of E such that $H \subset p^{e_p}\mathbb{Z}_p$ (we take $e_p = \infty$ e.g. if $H = \{0\}$). This gives a map from the set of closed subgroups of $\widehat{\mathbb{Z}}$ to the set of supernatural numbers by $H \mapsto \prod_p p^{e_p(H)}$. It is now easy to see that

$$m\widehat{\mathbb{Z}} \mapsto \prod_{n} p^{e_p(m\widehat{\mathbb{Z}})} = m$$

under this map; therefore the map $m \mapsto m\widehat{\mathbb{Z}}$ has a right inverse, so it is surjective as well.

Problem R3. Let K and L be extensions of a field k inside a large field Ω (as in Chapter VIII, §3). Is it true that K and L are linearly disjoint over k if and only if the natural map $K \otimes_k L \to \Omega$ is injective?

Solution. Yes, this statement is true. First suppose K and L are linearly disjoint. Let

$$\alpha = \sum_{i} x_i \otimes y_i \in K \otimes_k L$$

be any element. By k-bilinearity of the tensor product, we may assume that the x_i are linearly independent over k, for e.g. if $x_j = \sum_i \alpha_i x_i$, then

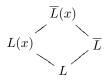
$$x_j \otimes y_j = \sum_i x_i \otimes (\alpha_i y_j).$$

Then since K and L are linearly disjoint, the x_i are linearly independent over L, so if $\alpha \mapsto 0 = \sum_i x_i y_i$, we have $y_i = 0$ for all i, hence $\alpha = 0$.

Conversely, let $x_1, \ldots, x_n \in K$ be linearly independent over k. Suppose that there exist $y_i \in L$ such that $\sum_i x_i y_i = 0 \in \Omega$; then $\sum_i x_i \otimes y_i \mapsto 0$, so by injectivity, we have $\sum_i x_i \otimes y_i = 0$. Since $x_i \in K$ are linearly independent over k, the elements $x_i \otimes 1 \in K \otimes L$ are linearly independent over L, a contradiction.

Problem R4. At the beginning of the proof of Theorem VIII.4.13, Lang says, "From the hypotheses, we deduce that K is free from the algebraic closure L^a of L over k." How do we deduce this?

Solution. Let $x_1, \ldots, x_n \in K$ be algebraically independent over k, in other words, trdeg(k(x)/k) = n. We know that K is free from L over k, so trdeg(L(x)/L) = n. We have the following diagram of fields:



By problem 3 (proven below, without using this result),

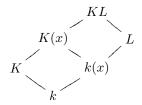
$$\operatorname{trdeg}(\overline{L}(x)/L) = \operatorname{trdeg}(\overline{L}(x)/L(x)) + \operatorname{trdeg}(L(x)/L) = 0 + n = n$$

since $\operatorname{trdeg}(\overline{L}(x)/L(x)) \leq \operatorname{trdeg}(\overline{L}/L) = 0$. So x_1, \ldots, x_n are also algebraically independent over \overline{L} .

Problem 2. A subfield k of a field K is said to be algebraically closed in K if every element of K which is algebraic over k is contained in k. Prove: If k is algebraically closed in K, and K, L are free over k, and L is separable over k or K is separable over k, then L is algebraically closed in KL.

Solution. If K is separable over k, then K/k is a regular extension, so by Theorem 4.13, KL/L is regular and in particular, L is algebraically closed in L.

So we suppose that L is separable over k. We may assume that L is finitely generated over k. Let x_1, \ldots, x_n be a separating transcendence base for the extension L over k, so that L is a finite separable extension of $k(x) = k(x_1, \ldots, x_n)$. Since the x_i are algebraically independent over k and L is free from K, we know that k is algebraically closed in K(x), so k(x) is algebraically closed in K(x). We therefore reduce to the case where L is a finite separable extension of k.



Suppose that $\alpha \in KL$ is algebraic over L. By the proof of Lemma 4.10, the minimal polynomial of α over k remains irreducible over K, and hence is minimal. But since L is separable over k, we have by Corollary 4.5 that KL is separable over K, therefore the minimal polynomial of α must be separable over K, so α is in fact separable over k. Therefore $L(\alpha)$ is finite and separable, so it is primitively generated; by Lemma 4.10 we have

$$[L(\alpha):k] = [KL(\alpha):K] = [KL:K] = [L:k]$$

so $L = L(\alpha)$.

Note that we do in fact need the assumption that L is separable over k. For example, take $k = \mathbb{F}_p(x, y)$, K = k(u, v) where u and v are independent transcendentals related by the equation $xu^p - yv^p = 1$, and $L = k(x^{1/p})$. One can check that k is algebraically closed in K. Since L is algebraic over k, L is free from K. Then in KL we have the equation

$$y = \frac{xu^p - 1}{v^p} = \left(\frac{x^{1/p}u - 1}{v}\right)^p$$

and $KL \supset L(y^{1/p}) \supset L$.

Problem 3. Let $k \subset E \subset K$ be extension fields. Show that

$$\operatorname{trdeg}(K/k) = \operatorname{trdeg}(K/E) + \operatorname{trdeg}(E/k)$$

Show if $\{x_i\}$ is a transcendence base of E/k, and $\{y_j\}$ is a transcendence base of K/E, then $\{x_i, y_j\}$ is a transcendence base of K/k.

Solution. We prove the second statement; the first statement follows. Since $\{x_i\}$ is a transcendence basis of E/k, by definition E is algebraic over k(x); the class of algebraic extensions is distinguished (§V.1), so E(y) is algebraic over k(x, y) and K is algebraic over E(y) so K is algebraic over k(x, y). Thus

$$\operatorname{trdeg}(K/k) \le \#\{x_i, y_j\},\$$

and it suffices to show that the set $\{x_i, y_j\} \subset K$ is algebraically independent, for then

$$\operatorname{trdeg}(K/k) \ge \#\{x_i, y_j\} = \#\{x_i\} + \#\{y_j\} = \operatorname{trdeg}(E/k) + \operatorname{trdeg}(K/E)$$

Suppose that

$$f(x_i, y_j) = \sum_{I J} a_{IJ} x^I y^J = 0$$

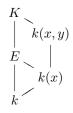
is an algebraic dependence relation with $a_{IJ} \in k$ and x^I , y^J monomials in the x_i, y_j , respectively. Since y_j are algebraically independent over E, viewing f as a polynomial in the y_j we see that f must be of the form

$$f(x_i) = \sum_I a_I x^I = 0;$$

but then again the x_i are algebraically independent over k, so this polynomial is identically zero.

Problem 4. Let K/k be a finitely generated extension, and let $K \supset E \supset k$ be a subextension. Show that E/k is finitely generated.

Solution. Let $\{x_i\}$ be a transcendence base for E/k and $\{y_j\}$ for K/E. By the previous exercise, we see that each of these sets is finite and that K is algebraic over k(x, y). Since K is finitely generated, K is finitely generated algebraic over k(x, y), hence $[K : k(x, y)] < \infty$.



It suffices to show that E is finitely generated over k(x); we will show it is finite. From Proposition 3.3, the field k(x, y) is linearly disjoint from E (since y_j are algebraically independent). Thus if $\{u_m\} \subset E$ is linearly independent over k(x) it remains so over k(x, y), hence $\#\{u_m\} \leq [K : k(x, y)] < \infty$ and the claim follows.

Problem 5. Let k be a field and $k(x_1, \ldots, x_n) = k(x)$ be a finite separable extension. Let u_1, \ldots, u_n be algebraically independent over k. Let

$$w = u_1 x_1 + \dots + u_n x_n.$$

Let $k(u) = k(u_1, ..., u_n)$. Show that k(u)(w) = k(u)(x).

Solution. The inclusion $k(u)(w) \subset k(u)(x)$ is clear.

Let K be the normal closure of k(x) in a fixed algebraic closure; by §V.4, the extension K/k is also finite, separable. Let d = [k(x) : k], and let $\sigma_i : k \hookrightarrow K$ be the d distinct embeddings of k into K. By Proposition 3.3 and Lemma 4.10, the extensions k(u) (pure transcendental) and K (finite, separable, hence singly generated) are linearly disjoint over k hence free, and [k(u)(x) : k(u)] = d. But we have $\sigma_i(w) \neq \sigma_j(w)$ for all $i \neq j$, since otherwise

$$\sum_{m} \left(\sigma_i(x_m) - \sigma_j(x_m) \right) u_m = 0 \in K(u),$$

so by freeness $\sigma_i(x_m) = \sigma_j(x_m)$ for all m, a contradiction. Therefore the minimal polynomial of w is degree $\geq d [k(x)(u) : k(u)] \geq d$, which completes the proof.

Problem 6. Let $k(x) = k(x_1, \ldots, x_n)$ be a separable extension of transcendence degree $r \ge 1$. Let u_{ij} (with $i = 1, \ldots, r$, $j = 1, \ldots, n$) be algebraically independent over k(x). Let

$$y_i = \sum_{j=1}^n u_{ij} x_j$$

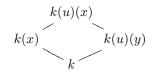
Let $k(u) = k(u_{ij})_{i,j}$.

- (a) Show that k(u)(x) is separable algebraic over $k(u)(y_1, \ldots, y_r) = k(u)(y)$.
- (b) Show that there exists a polynomial $P(u) \in k[u]$ having the following property: Let $(c) = (c_{ij})$ be elements of k such that $P(c) \neq 0$. Let

$$y_i' = \sum_{j=1}^n c_{ij} x_j.$$

Then k(x) is separable algebraic over k(y').

Solution. We have the following diagram of fields:



The extension k(u)(x) of k(x) is separable since the u_{ij} are algebraically independent over k(x). By assumption, k(x) is separable over k, so by Corollary 4.3, k(u)(x) is separable over k. Therefore by Corollary 4.2, k(u)(x) is separable over k(y).

By Problem 3, we have

$$\operatorname{trdeg}(k(u)(x)/k) = \operatorname{trdeg}(k(u)(x)/k(x)) + \operatorname{trdeg}(k(x)/k) = rn + r$$

since the u_{ij} are algebraically independent. Therefore

$$rn + r = \operatorname{trdeg}(k(u)(x)/k(u)(y)) + \operatorname{trdeg}(k(u)(y)/k(u)) + \operatorname{trdeg}(k(u)/k);$$

since u_{ij} are algebraically independent over k(x) they are so over k, and we conclude that $\operatorname{trdeg}(k(u)/k) = rn$, and it suffices to prove that $\operatorname{trdeg}(k(u)(y)/k(u)) = r$. If not, there exists an algebraic dependence $\sum_{I} a_{I} y^{I} = 0$ with the $a_{I} \in k(u)$ and y^{I} a monomial in the y_{j} . By clearing denominators, we can write this as $\sum_{I} b_{I} u^{I} = 0$ with $b_{I} \in k(y)$ and u^{I} monomials in u_{j} . Expanding this relation in the x_{i} gives a relation $\sum_{I} b'_{I} u^{I} = 0$ with $b_{I} \in k(x)$, a contradiction as the x_{i} are algebraically independent over k(u).

Part (b) follows from Corollary 2.3 and part (a).

Problem 7. Let k be a field and $k[x_1, \ldots, x_n] = R$ a finitely generated entire ring over k with quotient field k(x). Let L be a finite extension of k(x). Let I be the integral closure of R in L. Show that I is a finite R-module. [Hint: Use Noether Normalization, and deal with the inseparability problem and the separable case in two steps.]

Solution. By Proposition V.6.6, we have $L \supset L_0 \supset k(x)$ where L is purely inseparable over L_0 and L_0 is separable over k(x). By Noether normalization (Theorem VIII.2.1), there exist $y_1, \ldots, y_r \in R$ such that R is integral over $k[y_1, \ldots, y_r]$. Let $k(y) = k(y_1, \ldots, y_r)$ and $k[y] = k[y_1, \ldots, y_r]$. We have the following diagram:

$$\begin{array}{cccc} I & L \\ {}^{|} & {}^{|} \\ I_0 & L_0 \\ {}^{|} & {}^{|} \\ R & k(x) \\ {}^{|} & {}^{|} \\ k[y] & k(y) \end{array}$$

First, assume that R is integrally closed in k(x). Then the fact that I_0 is a finite R-module follows from Exercise VII.3. For the inseparable extension, it suffices to treat the case where $L = L_0(t^{1/p})$ where $t \in L_0 \setminus L_0^p$. Let $\alpha = a_0 + \cdots + a_{p-1}(t^{1/p})^{p-1} \in L$ be integral over L_0 ; the minimal polynomial of α is $X^p = a_0^p + \cdots + a_{p-1}t^{p-1}$ so $a_i^p \in I_0$ for each i. Since I_0 is integrally closed, $a_i \in I_0$, hence $I = I_0[t^{1/p}]$.

The general case now follows by applying the statement with L = K (since k[y] is integrally closed in k(y)): if I is a finite k[y]-module and R is a finite k[y]-module, then I is a finite R-module.