Math 212 MT
Apr 11th, 2009
Ali Nesin

1. *Show that any ring endomorphism from a field into a ring is one-to-one*. (2 pts.)
Proof: A field has no nontrivial ideals, so the kernel of an endomorphism is either 0 or R. But 1 is not in the kernel, so that the kernel is trival and the endomorphism is one-to-one.

2. *Let F be a field of prime characteristic p.*

2a. *Show that* $x \mapsto x^p$ *is a ring endomorphism of F*. (3 pts.)

Proof: This follows from the elementary fact that if $0 < i < p$ then p divides $\binom{p}{i}$.

2b. *Show that if F is finite this endomorphism is always an automorphism.* (3 pts.)
Proof: The endomorphism is one-to-one by #1. So it is onto as well.

2c. *Find a field F of characteristic p where this endomorphism is not an automorphism.* (5 pts.)

Answer: Let $K = \mathbb{Z}/p\mathbb{Z}$ and $F = K(X)$.

3. *Let R be a domain and* $a \in R^*$ *and* $b \in R$.

3a. *Show that the map defined by the formula* $f(X) \mapsto f(aX + b)$ *is an automorphism of* $R[X]$. (4 pts.)

Proof: The map is obviously an endomorphism of $R[X]$, say φ. Consider the endomorphism $f(X) \mapsto f(a^{-1}X - a^{-1}b)$ of $R[X]$. Call it ψ. Then $(\psi \circ \varphi)(X) = \psi(\varphi(X)) = \psi(aX + b) = a(a^{-1}X - a^{-1}b) + b = X$. Hence $\psi \circ \varphi = \mathrm{Id}_{R[X]}$. Similarly $\varphi \circ \psi = \mathrm{Id}_{R[X]}$.

3b. *Show that this is not so if* $a \in R \setminus R^*$. (4 pts.)

Proof: Assume $f(X) \mapsto f(aX + b)$ is an automorphism of $R[X]$. We know from above that the map $f(X) \mapsto f(X - b)$ is an automorphism of $R[X]$. Composing these two, we see that the map $f(X) \mapsto f(aX)$ is an automorphism of $R[X]$. But then, the leading coefficient of any nonconstant polynomial is a multiple of a. Thus a is invertible.

4. *Let R be a domain and* $f \in R[X]$. *Consider the subring* $R[f]$ of $R[X]$ *generated by R and f. Find a necessary and sufficent condition on f for* $R[X] = R[f]$. (6 pts.)
Answer: Clearly $R[f] \leq R[X]$. Now, $R[X] = R[f]$ iff $X \in F[f]$ iff $X = g(f)$ for some polynomial g over F. Comparing degrees, we get $1 = (\deg f)(\deg g)$. Thus $\deg f = 1 = \deg g$. Writing $f(X) = aX + b$ and $g(X) = cX + d$, we get $X = g(f) = c(aX + b) + d$, so that $ca = 1$ and hence $a \in R^*$. Conversely if $f(X) = aX + b$ with $a \in R^*$ and $b \in R$, then, from the previous question we get $R[f] = R[X]$

5. *Find* $\mathrm{Aut}(R[X] : R) = \{$*automorphisms of* $R[X]$ *that fix R pointwise*$\}$. (4 pts.)
Answer: Let $\varphi \in \mathrm{Aut}(R[X] : R)$. Then φ is given by the image of X. Say $\varphi(X) = f$. Then $R[X] = \mathrm{Im}\ \varphi = R[f]$. By question 4, $f(X) = aX + b$ for some $a \in R^*$ and $b \in R$. By question 3, all such endomorphisms are automorphisms of $R[X]$ over R.

6. *Let C be the set of functions from $\mathbb{R}$ into $\mathbb{R}$. Then C is a ring under the addition and multiplication of functions.*

6a. *Describe the invertible elements of C.* (2 pts.)

Answer: $C^* = \{f : \mathbb{R} \to \mathbb{R} : f(x) \neq 0$ for any $x\}$.

6b. *Describe the set of zero divisors of C.* (2 pts.)

Answer: $\{f : \mathbb{R} \to \mathbb{R} : f(x) = 0$ for some $x\}$.

6c. *Let $a \in \mathbb{R}$ be fixed. Consider $I_a = \{f \in C : f(a) = 0\}$. Show that I_a is a maximal ideal of C. Find the isomorphism type of the ring C/I_a.* (6 pts.)

Answer: Consider the map $C \to \mathbb{R}$ defined by $f \mapsto f(a)$. This is a ring endomorphism which is clearly onto and whose kernel is I_a. Thus $C/I_a \approx \mathbb{R}$ is a field, so that I_a is a maximal ideal.

6d. *Show that there is a maximal ideal of C different from all I_a.* (7 pts.)

Answer: Let $J = \{f \in C : f(x) \neq 0$ for only finitely many $x \in \mathbb{R}\}$. Then $J \lhd C$ and $J \not\subset I_a$. By Zorn's Lemma there is a maximal $\mathfrak{m}$ ideal containing J. If $\mathfrak{m} = I_a$ for some $a \in \mathbb{R}$, then $J \subseteq \mathfrak{m} = I_a$, a contradiction.

7. *Let F be a field and R a domain containing F. Show that if* $\dim_F(R)$ *is finite, then R is a field.* (6 pts.)

Proof: Let $a \in R \setminus \{0\}$. Let $m : R \to R$ be defined by $m(x) = ax$. Then m is an F-vector space homomorphism. Since R is a domain, Ker $m = \mathrm{ann}_R\, x = 0$, so that m is one-to-one. Since R is a finite dimensionl vector space, this implies that m is onto.

8. *Let R be a UFD and K its field of fractions. Let $f \in R[X]$. Show that if f is irreducible in $R[X]$ then it is irreducible in $K[X]$.* (5 pts.)

Proof: Let $f = gh$ for $g, h \in K[X]$. We can write $g = g'/r$, $h = h'/s$ where $g', h' \in R[X]$ are R-scalar multiples of g and h respectively and $r, s \in R$. Therefore $rsf = g'h'$. By Gauss Lemma, any prime that divides r or s divides either g' or h'. By induction rs divides g' and h'. So $f = g''h''$ for $g'', h'' \in R[X]$. Thus either g'' or h'' is in R, i.e. its degree is 0. So the same holds for g or h.

9. *Let F be a field and $f, g \in F[X] \setminus \{0\}$ be two nonzero polynomials. Show that f/g is algebraic over F if and only if $f/g \in F$. Conclude that if f or g are not both constant polynomials then $F[f/g] \approx F[X]$.* (5 pts.)

Proof: We may assume that f and g are prime to each other. Assume there are constants $a_i \in F$ such that

$$a_0 + a_1 f/g + a_2 f^2/g^2 + \ldots + a_2 f^n/g^n = 0.$$

We may assume that a_0 and $a_n \neq 0$. Then

$$a_0 g^n + a_1 f g^{n-1} + a_2 f^2 g^{n-2} + \ldots + a_2 f^n = 0.$$

It follows that any prime factor of f divides g and vice versa. So f and g must be in F.

10. *Let F be a field and $g(Z), f(Z) \in F[Z]$ be two nonzero polynomials which are prime to each other. Show that the polynomial $g(Z) - Yf(Z)$ of $F[Y, Z]$ is prime in $F[Y, Z]$. Conclude that the polynomial $g(Z) - Yf(Z)$* of *$F(Y)[Z]$ is prime in $F(Y)[Z]$.* (8 pts.)

Proof: Assume $g(Z) - Yf(Z) = h(Y, Z)k(Y, Z)$. Then $\deg_Y h + \deg_Y k = 1$. Assume $\deg_Y h = 1$ and $\deg_Y k = 0$. Then $h(Y, Z) = a(Z) + b(Z)Y$ and $k(Y, Z) = k(Z)$. Therefore we have $g(Z) - Yf(Z) = (a(Z) + b(Z)Y)\, k(Z)$ and so $a(Z)k(Z) = g(Z)$ and $b(Z)k(Z) = f(Z)$. Since f and g are prime to each other, $k(Y, Z) = k(Z) = k \in F$. The second part follows from # 8.

11. *Let F be a field. We let $K = F(Y)$ where Y is an indeterminate.*

11a. *Consider the subrings $F[Y^2]$ and $F[Y]$ of K. Show that $F[Y^2] \approx F[Y]$. What is $[F(Y) : F(Y^2)]$?* (8 pts.)

Proof: We know that Y^2 is transcendental over F, so $F[Y^2] \approx F[Y]$. (The map $f(Y) \mapsto f(Y^2)$ is the required isomorphism.)

Y is the root of the polynomial $p(Z) = Z^2 - Y^2$ over the field $F(Y^2)$ which is of degree 2. Let us show that this polynomial is irreducible $F(Y^2)[Z]$. By #8 it is enough to show this in $F[Y^2, Z]$. Otherwise there are polynomials $a(Y^2)$, $b(Y^2)$, $c(Y^2)$, $d(Y^2) \in F[Y^2]$ such that

$$p(Z) = Z^2 - Y^2 = (a(Y^2) + Zb(Y^2))(c(Y^2) + Zd(Y^2)).$$

Thus $b(Y^2)d(Y^2) = 1$ and so $b(Y^2) = b \in F$ and $d(Y^2) = d \in F \in F$. Also $a(Y^2)c(Y^2) = Y^2$; thus, say, $a(Y^2) = \alpha Y^2$ and $c(Y^2) = c \in F$. Thus

$$p(Z) = Z^2 - Y^2 = (\alpha Y^2 + Zb)(c + Zd).$$

Since there are no terms in Y^2Z on the LHS, clearly α must be 0. The rest is easy. Thus $p(Z) = Z^2 - Y^2$ is the minimal polynomial of Y over $F(Y^2)$ and so,

$F(Y) = F(Y^2)(Y) = F(Y^2)[Y] = F(Y^2)[Z]/\langle p\rangle$

And it has degree = deg $p = 2$.

11b. *Consider the subrings $F[Y^2]$ and $F[Y]$ of K. Show that $F[1/Y^3] \approx F[Y]$. What is $[F(Y) : F(1/Y^3)]$?* (*Only outline the proof.*) (3 pts.)

Proof: Note that $F(1/Y^3) = F(Y^3)$. The rest can be done as above. The answer is 3. It also follows from 12b.

12. *Let F be a field. Let X be an indeterminate over F.*

12a. *Let f, $g \in F[X]$ be such that $f/g \notin F$. Let $Y = f/g \in F(X)$. Show that* $[F(X) : F(Y)] \leq \max\{\deg f, \deg g\}$. (6 pts.)

Proof: Clearly X is the root of the polynomial $g(Z)Y - f(Z) \in F(Y)[Z]$. Thus the minimal polynomial of X over $F(Y)$ divides $g(Z)Y - f(Z)$, whose degree in X is $\max\{\deg g, \deg f\}$. Thus the degree of the minimal polynomial of X over $F(Y)$ is less than or equal to $\max\{\deg g, \deg f\}$, that is $[F(X) : F(Y)] \leq \max\{\deg f, \deg g\}$.

12b. *Let f, g and Y be as above and f and g are coprime. Show that* $[F(X) : F(Y)] = \max\{\deg f, \deg g\}$. (10 pts.)

Proof: We need to show that the polynomial $g(Z)Y - f(Z)$ of $F(Y)[Z]$ is irreducble in $F(Y)[Z]$. Noting that $g(Z)Y - f(Z)$ of $F[Y][Z]$, by #8, it is enough to show that the polynomial $g(Z)Y - f(Z)$ is irreducible in $F[Y][Z] = F[Y, Z]$. Suppose, $g(Z)Y - f(Z) = p(Y, Z)\, q(Y, Z)$. By comparing degrees in Y we see that, say,

$$p(Y, Z) = p(Z) \text{ and } q(Y, Z) = a(Z) + b(Z)Y$$

for some polynomails $a(Z)$, $b(Z) \in K[Z]$. Thus

$$g(Z)Y - f(Z) = p(Z)(a(Z) + b(Z)Y) = p(Z)a(Z) + p(Z)b(Z)Y$$

and so $g(Z) = p(Z)b(Z)$ and $f(Z) = p(Z)a(Z)$. Since f and g are coprime, this implies that $p(Z) = p \in K$.

13. Conclude from above that for any $\varphi \in \mathrm{Aut}(F(X)/F)$ there are $a, b, c, d \in F$ such that $\varphi(X) = \dfrac{aX+b}{cX+d}$. Show that we must have $ad - bc \neq 0$. (10 pts.)

Proof: Easy by now!