

## ALGEBRA HW 7

CLAY SHONKWILER

1

Which of the following rings  $R$  are discrete valuation rings? For those that are, find the fraction field  $K = \text{frac } R$ , the residue field  $k = R/\mathfrak{m}$  (where  $\mathfrak{m}$  is the maximal ideal), and a uniformizer  $\pi$ . For the others, explain why not.  $\mathbb{Z}$ ,  $\mathbb{Z}_{(5)}$ ,  $\mathbb{Z}[1/5]$ ,  $\mathbb{R}[x]$ ,  $\mathbb{R}[x]_{(x-2)}$ ,  $\mathbb{R}[x, 1/(x-2)]$ ,  $\mathbb{Q}[x]_{(x^2+1)}$ ,  $\mathbb{C}[x, y]_{(x, y)}$ ,  $(\mathbb{R}[x, y]/(x^2 + y^2 - 1))_{(x-1, y)}$ ,  $(\mathbb{R}[x, y]/(y^2 - x^3))_{(x, y)}$ .

**Answer:**  $\mathbb{Z}$ :  $\mathbb{Z}$  is not a d.v.r., since  $\mathbb{Z}$  has maximal ideals  $(p)$  for  $p$  prime; that is,  $\mathbb{Z}$  is not a local ring.

$\mathbb{Z}_{(5)}$ :  $\mathbb{Z}_{(5)}$  is a d.v.r., with maximal ideal  $\mathfrak{m} = (5)$ . The uniformizer is  $\pi = 5$ , since every ideal is of the form  $(5^a)$ . The fraction field  $K = \text{frac } \mathbb{Z}_{(5)}$  is

$$K = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}_{(5)}, b \neq 0 \right\} = \mathbb{Q}.$$

Finally, the residue field is

$$k = \mathbb{Z}_{(5)}/(5) = \mathbb{Z}/5.$$

$\mathbb{Z}[1/5]$ :  $\mathbb{Z}[1/5]$  is not a d.v.r., since  $\mathbb{Z}[1/5]$  has maximal ideals  $(p)$  where  $p$  prime and  $p \neq 5$ ; that is,  $\mathbb{Z}[1/5]$  is not local.

$\mathbb{R}[x]$ :  $\mathbb{R}[x]$  is not a d.v.r., since  $(x - a)$  is a maximal ideal of  $\mathbb{R}[x]$  for all  $a$ ; that is,  $\mathbb{R}[x]$  is not a local ring.

$\mathbb{R}[x]_{(x-2)}$ :  $\mathbb{R}[x]_{(x-2)}$  is a d.v.r., with maximal ideal  $\mathfrak{m} = (x - 2)$ . The uniformizer is  $\pi = x - 2$ . The fraction field  $K = \text{frac } \mathbb{R}[x]_{(x-2)}$  is

$$K = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{R}[x]_{(x-2)}, g(x) \neq 0 \right\} = \mathbb{R}(x).$$

The residue field is

$$k = \mathbb{R}[x]_{(x-2)}/(x - 2) = \mathbb{R}.$$

$\mathbb{R}[x, 1/(x - 2)]$ : This is not a d.v.r., since, in  $\mathbb{R}[x, 1/(x - 2)]$ ,  $(x - a)$  is a maximal ideal for  $a \neq 2$ ; that is,  $\mathbb{R}[x, 1/(x - 2)]$  is not a local ring.

$\mathbb{Q}[x]_{(x^2+1)}$ : This is a d.v.r., with maximal ideal  $\mathfrak{m} = (x^2 + 1)$ . The uniformizer is  $\pi = x^2 + 1$ . The fraction field  $K = \text{frac } \mathbb{Q}[x]_{(x^2+1)}$  is

$$K = \left\{ \frac{f}{g} : f, g \in \mathbb{Q}[x]_{(x^2+1)}, g \neq 0 \right\} = \mathbb{Q}[x]_{(x^2+1)} \left( \frac{1}{x^2 + 1} \right) = \mathbb{Q}(x).$$

The residue field is

$$k = \mathbb{Q}[x]_{(x^2+1)}/(x^2 + 1) = \mathbb{Q}[i].$$

$\mathbb{C}[x, y]_{(x, y)}$ :  $\mathbb{C}[x, y]_{(x, y)}$  is not a d.v.r., since it is not dimension 1; specifically, it is dimension 2.

$(\mathbb{R}[x, y]/(x^2 + y^2 - 1))_{(x-1, y)}$ : This ring is a d.v.r., with maximal ideal  $\mathfrak{m} = (y)$ . This is because  $x + 1 \notin (x - 1, y)$ , so  $\frac{1}{x+1} \in R$  and

$$x - 1 = \left( \frac{(x+1)(x-1)}{x+1} \right) = \left( \frac{x^2 - 1}{x+1} \right) = \frac{-y^2}{x+1} = \left( \frac{-y}{x+1} \right) y \in (y).$$

Hence,  $(x - 1, y) = (y)$ , so  $R$  is a d.v.r. with uniformizer  $\pi = y$ . Now,  $\mathbb{R}(y)$  injects into  $R$  and  $\mathbb{R}(y)[x]/(x^2 + y^2 - 1)$  contains  $R$ . Since  $x^2 + (y^2 - 1)$  is irreducible in  $\mathbb{R}(y)[x]$ ,  $\mathbb{R}(y)[x]/(x^2 + y^2 - 1)$  is a field and so contains the fraction field  $K = \text{frac } R$ . Now,  $K \supseteq \mathbb{R}(y)$  so, since  $\mathbb{R}(y)[x]/(x^2 + y^2 - 1)$  is a quadratic extension of  $\mathbb{R}(y)$ , we see that either  $K = \mathbb{R}(y)$  or  $K = \mathbb{R}(y)[x]/(x^2 + y^2 - 1)$ . Clearly,  $R \not\subseteq \mathbb{R}(y)$ , so we conclude that

$$K = \mathbb{R}(y)[x]/(x^2 + y^2 - 1).$$

The residue field is

$$k = (\mathbb{R}[x, y]/(x^2 + y^2 - 1))_{(x-1, y)} / (y) = \mathbb{R}[x]/(x-1) = \mathbb{R}.$$

$(\mathbb{R}[x, y]/(y^2 - x^3))_{(x, y)}$ : As we saw in class,  $z = \frac{x}{y}$  is in the integral closure of  $R$ , but is not contained in  $R$ , so  $R$  is not integrally closed and, therefore, not a d.v.r.



## 2

Let  $R$  be a discrete valuation ring with fraction field  $K$ , maximal ideal  $\mathfrak{m}$ , and discrete valuation  $v$ . If  $a, b \in K$ , define  $\rho(a, b) = 2^{-v(a-b)}$  if  $a \neq b$ , and define  $\rho(a, a) = 0$ .

**(a):** Show that  $\rho$  defines a metric on  $K$ .

*Proof.* Suppose  $\rho(a, b) = 0$ . Then  $2^{-v(a-b)} = 0$  or  $a = b$ . However, since  $2^c > 0$  for all  $c \in \mathbb{Z}$ , only the latter case obtains, so  $a = b$ . On the other hand, by definition,  $\rho(a, a) = 0$ .

To show symmetry, note first that symmetry is trivial in the case that  $a = b$ . Thus, suppose  $\pi$  is the uniformizer of the discrete valuation. Then, for  $a, b \in K$ ,  $a \neq b$ ,

$$a - b = u\pi^n$$

where  $u \in R^*$  and  $v(a - b) = n$ . Then

$$b - a = -(a - b) = -u\pi^n;$$

since  $-u \in R^*$ ,  $v(b - a) = n = v(a - b)$ . Hence,

$$\rho(a, b) = 2^{-v(a-b)} = 2^{-v(b-a)} = \rho(b, a),$$

so  $\rho$  is symmetric.

To see that  $\rho$  satisfies the triangle inequality, suppose  $a, b, c \in K$ . If  $b = a$  or  $b = c$ , the triangle inequality is trivial, so suppose that  $b \neq a$  and  $b \neq c$ . Similarly if  $a = c$ , then the triangle inequality is trivial, so assume  $a \neq c$ . Then

$$v(a - c) = v(a - b + b - c) \geq \min\{v(a - b), v(b - c)\},$$

so  $2^{-v(a-c)} \leq \max\{2^{-v(a-b)}, 2^{-v(b-c)}\}$ . Hence, since  $2^n > 0$  for all  $n \in \mathbb{Z}$ ,

$$\rho(a, c) = 2^{-v(a-c)} \leq 2^{-v(a-b)} + 2^{-v(b-c)} = \rho(a, b) + \rho(b, c).$$

□

**(b):** Show that  $\rho$  is an ultrametric (=non-archimedean metric); i.e., it satisfies the strong triangle inequality  $\rho(a, c) \leq \max\{\rho(a, b), \rho(b, c)\}$ .

*Proof.* Let  $a, b, c \in K$ . If  $a = c$ , then  $\rho(a, c) = 0 \leq \max\{\rho(a, b), \rho(b, c)\}$  trivially. If  $b = a$  or  $b = c$  then this statement is trivial, so assume  $b \neq a, b \neq c, a \neq c$ . Then in part (a) we saw that

$$\rho(a, c) = 2^{-v(a-c)} \leq \max\{2^{-v(a-b)}, 2^{-v(b-c)}\} = \max\{\rho(a, b), \rho(b, c)\}.$$

□

**(c):** Show that  $(K, \rho)$  is a topological field, i.e. that it is a topological space in which addition and multiplication define continuous maps  $K \times K \rightarrow K$ .

*Proof.*  $K$  is certainly a topological space under the metric topology, and  $K \times K$  is a topological space under the product topology. Let  $(a, b) \in K \times K$  and let  $\epsilon > 0$ . If  $(c, d) \in K \times K$  such that  $0 < \rho(a, c) < \epsilon$  and  $0 < \rho(b, d) < \epsilon$ , then, if  $a + b \neq c + d$ ,

$$\begin{aligned} \rho(a + b, c + d) &= 2^{-v((a+b)-(c+d))} = 2^{-v((a-c)+(b-d))} \\ &\leq \max\{2^{-v(a-c)}, 2^{-v(b-d)}\} \\ &= \max\{\rho(a, c), \rho(b, d)\} \\ &< \epsilon. \end{aligned}$$

Obviously if  $a + b = c + d$ , then  $\rho(a + b, c + d) = 0 < \epsilon$ . Therefore, since our choice of  $\epsilon > 0$  was arbitrary, we see that the function defined by addition is continuous at  $(a, b)$ . Since our choice of  $(a, b)$  was arbitrary, this implies that addition, as a map  $K \times K \rightarrow K$ , is continuous.

Turning to multiplication, again let  $(a, b) \in K \times K$  and let  $\epsilon > 0$ . Let  $\delta_1 = \frac{\epsilon}{\max\{1, \rho(b, 0)\}}$  and let  $\delta_2 = \frac{\epsilon}{\max\{\delta_1, \rho(a, 0)\}}$ . Now, if  $(c, d) \in K \times K$  such that  $\rho(a, c) < \delta_1$  and  $\rho(b, d) < \delta_2$ , then, so long as  $ab \neq cd$  (if  $ab = cd$  then  $\rho(ab, cd) = 0 < \epsilon$ ),

$$(1) \quad \rho(ab, cd) \leq \max\{\rho(ab, cb), \rho(bc, cd)\}.$$

Now, if  $ab = cb$ , then  $\rho(ab, cb) = 0 < \epsilon$ . If  $ab \neq cb$ , then  $b \neq 0$  and  $a \neq c$ . Hence,

$$\begin{aligned}
 \rho(ab, cb) &= 2^{-v(ab-cb)} = 2^{-v(b(a-c))} = 2^{-(v(b)+v(a-c))} \\
 &= 2^{-v(b)} \cdot 2^{-v(a-c)} \\
 &= \rho(b, 0) \cdot \rho(a, c) \\
 &< \rho(b, 0)\delta_1 \\
 &< \rho(b, 0)\frac{\epsilon}{\rho(b, 0)} \\
 &= \epsilon.
 \end{aligned}
 \tag{2}$$

Thus,  $\rho(ab, cb) < \epsilon$ .

On the other hand, if  $bc = cd$ , then  $\rho(bc, cd) = 0 < \epsilon$ . If  $bc \neq cd$ , then  $c \neq 0$  and  $b \neq d$ . Hence,

$$\begin{aligned}
 \rho(bc, cd) &= 2^{-v(bc-cd)} = 2^{-v(c(b-d))} \\
 &= 2^{-(v(c)+v(b-d))} \\
 &= 2^{-v(c)} \cdot 2^{-v(b-d)} \\
 &= \rho(c, 0) \cdot \rho(b, d) \\
 &\leq (\max\{\rho(c, a), \rho(a, 0)\}) \cdot \rho(b, d) \\
 &= (\max\{\delta_1, \rho(a, 0)\}) \cdot \rho(b, d) \\
 &< (\max\{\delta_1, \rho(a, 0)\}) \frac{\epsilon}{\max\{\delta_1, \rho(a, 0)\}} \\
 &= \epsilon.
 \end{aligned}
 \tag{3}$$

Thus,  $\rho(bc, cd) < \epsilon$ .

Therefore, combining (1), (2) and (3), we see that

$$\rho(ab, cd) \leq \max\{\rho(ab, cb), \rho(bc, cd)\} < \epsilon.$$

Since our choice of  $\epsilon$  was arbitrary, we see that the function from  $K \times K \rightarrow K$  defined by multiplication is continuous at  $(a, b)$ ; since our choice of  $(a, b)$  was arbitrary, we see that multiplication is continuous on all of  $K \times K$ .

Thus, having shown that  $K$  is a topological space and that addition and multiplication defined continuous functions  $K \times K \rightarrow K$ , we conclude that  $K$  is a topological field.  $\square$

**(d):** Show that in  $K$ , the closed unit disc about 0 is  $R$  and the open unit disc about 0 is  $\mathfrak{m}$ .

*Proof.* Recall that  $R = \{a \in K : v(a) \geq 0\}$ . Then, for any  $a \in R$ ,  $v(a) \geq 0$  and so  $2^{-v(a)} \leq 1$ .

$$\rho(0, a) = \rho(a, 0) = 2^{-v(a-0)} = 2^{-v(a)} \leq 1.$$

So  $R = \{a \in K : \rho(0, a) \leq 1\}$ , the closed unit disc in  $K$ . Now, the maximal ideal  $\mathfrak{m} = \{a \in R : v(a) > 0\}$ . Hence, if  $a \in \mathfrak{m}$ ,  $v(a) > 0$ , so  $2^{-v(a)} < 1$ , so

$$\rho(0, a) = \rho(a, 0) = 2^{-v(a-0)} = 2^{-v(a)} < 1.$$

Thus,  $\mathfrak{m} = \{a \in K : \rho(0, a) < 1\}$ , the open unit disc in  $K$ .  $\square$

## 3

Let  $K$  be a field and let  $f(x) \in K[x]$  be a non-zero polynomial of degree  $n$ .

**(a):** Show that if  $a \in K$  is a root of  $f$ , then  $(x - a)$  divides  $f(x)$  in  $K[x]$ .

*Proof.* We prove this by induction on the degree of  $f$ . Note that, since we're in a field, we may as well assume  $f$  is monic. If the degree of  $f$  is 1, then  $f(x) = x - b$ , so if  $a$  is a root of  $f$ ,

$$a - b = 0,$$

so  $a = b$ . Now, suppose that, if  $a$  is a root of  $f$  implies  $(x - a)$  divides  $f(x)$  for all polynomials such that  $\deg(f) = k$ . Then, if  $f(x) \in K[x]$  such that  $\deg(f) = k + 1$  and  $a$  is a root of  $f$ , then  $f(x) = x^{k+1} + c_k x^k + \dots + c_1 x + c_0$ . Consider the first step of the division algorithm:

$$\begin{array}{r} x^{n-1} \\ x - a \overline{) x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} \dots + c_1x + c_0} \\ \underline{x^n - ax^{n-1}} \phantom{+ \dots + c_1x + c_0} \\ (c_{n-1} - a)x^{n-1} + c_{n-2}x^{n-2} + \dots + c_1x + c_0 \end{array}$$

Now, let

$$g(x) = f(x) - x^k(x - a) = (c_k + a)x^k + c_{k-1}x^{k-1} + \dots + c_1x + c_0.$$

Then, if  $a$  is a root of  $f$ ,

$$g(a) = (c_k + a)a^k + c_{k-1}a^{k-1} + \dots + c_1(a) + c_0 = a^{k+1} + c_k a^k + \dots + c_1(a) + c_0 = f(a) = 0,$$

so  $a$  is also a root of  $g$ . Now, since  $\deg(g) = k$ , we know, by the induction hypothesis, that  $(x - a)$  divides  $g(x)$ , so  $g(x) = (x - a)h(x)$ . Therefore,

$$f(x) = x^k(x - a) + g(x) = x^k(x - a) + h(x)(x - a) = (x^k + h(x))(x - a),$$

so  $x - a$  divides  $f(x)$ .  $\square$

**(b):** Deduce that  $f$  has at most  $n$  roots in  $K$ .

*Proof.* Let  $a_1$  be a root of  $f$ . Then, by part (a),

$$f(x) = (x - a_1)f_1(x),$$

for some  $f_1(x) \in K[x]$  with  $\deg(f_1) = n - 1$ . Then, if  $a_2$  is another root of  $f$ , then  $a_2$  must also be a root of  $f_1$ , so

$$f(x) = (x - a_1)(x - a_2)f_2(x)$$

where  $\deg(f_2) = n - 2$ . Iterating this process, we see that we eventually factor  $f$  into a product of irreducibles; in this factorization, there can be at most  $n$  linear factors, and, thus, at most  $n$  associated roots of  $f$ . Since  $K[x]$  is a UFD, this factorization is unique up to multiplication by a constant, so  $f$  is not divisible by any linear factors not appearing in this factorization. Hence, if  $b$  is a root of  $f$ , then, by (a),  $x - b$  must divide  $f(x)$ , so it must already appear in this factorization. Therefore, we see that there are at most  $n$  roots of  $f$ .  $\square$

**(c):** Will the argument and conclusion of part (b) still hold if  $K$  is replaced by a division algebra? Explain.

**Answer:** If  $K$  is replaced by a division algebra, the result in part (b) no longer holds. To see why, consider the division algebra  $\mathbb{H}$  and the polynomial  $x^2 + 1$  in  $\mathbb{H}[x]$ . Then  $\pm i$ ,  $\pm j$  and  $\pm k$  are all roots of  $x^2 + 1$ , so this polynomial has at least six roots in  $\mathbb{H}$  despite only being of degree 2.

The reason (b) fails if  $K$  is replaced by a division algebra is that  $K[x]$  is not necessarily a UFD if  $K$  is a division algebra, and we definitely needed unique factorization in part (b).



#### 4

Let  $R$  be a commutative ring of characteristic  $p$  (where  $p$  is prime) and define  $F : R \rightarrow R$  by  $a \mapsto a^p$ .

**(a):** Show that  $F$  is a ring endomorphism.

*Proof.* Clearly,  $F(0) = 0^p = 0$  and  $F(1) = 1^p = 1$ . Now, if  $a, b \in R$ , then

$$F(ab) = (ab)^p = a^p b^p = F(a)F(b).$$

Also,

$$F(a+b) = (a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{p-1} a b^{p-1} + b^p = a^p + b^p = F(a) + F(b),$$

since  $\binom{p}{k}$  is a multiple of  $p$  for  $1 \leq k \leq p-1$ . Therefore, we see that  $F$  preserves the identities, addition and multiplication, so  $F : R \rightarrow R$  is an endomorphism.  $\square$

**(b):** If  $R$  is a field, determine which elements lie in the set  $\{a \in R \mid F(a) = a\}$ .

**Answer:** If  $a \in \{a \in R \mid F(a) = a\}$ , then  $a$  is a root of the polynomial  $x^p - x$ . On the other hand, roots of this polynomial are certainly in the set, so we see that

$$\{a \in R \mid F(a) = a\} = \{a \in R \mid a \text{ is a root of } x^p - x\}.$$

Now, by 3(b) above,  $x^p - x$  has at most  $p$  roots in  $K$ . On the other hand, since  $K$  is a field of characteristic  $p$ , it contains the prime field  $\mathbb{Z}/p$ . Now, if  $a \in \mathbb{Z}/p$ , then  $a = 1 + \dots + 1$ ; hence,

$$a^p = (1 + \dots + 1)^p = 1^p + (1 + \dots + 1)^p = \dots = 1^p + \dots + 1^p = 1 + \dots + 1 = a,$$

so  $a$  is a root of  $x^p - x$ . Thus, all elements of  $\mathbb{Z}/p$  are roots of this polynomial, so there are at least  $p$  roots (since there are  $p$  elements of  $\mathbb{Z}/p$ ). Therefore, we conclude that there are exactly  $p$  roots of  $x^p - x$  in  $R$ , the elements of  $\mathbb{Z}/p$ . So  $\mathbb{Z}/p = \{a \in R \mid F(a) = a\}$  where  $\mathbb{Z}/p$  is considered as contained in  $R$ .



**(c):** If  $R$  is a field, must  $F$  be injective? surjective?

**Answer:** If  $R$  is a field, then  $F : R \rightarrow R$  is an endomorphism by (a), so  $\ker F$  is an ideal of  $R$ . Certainly  $F(1) = 1$ , so  $\ker F \neq R$ ; the only other ideal of  $R$  is  $(0)$ , so  $\ker F = (0)$ . Hence,  $F$  is injective.

On the other hand, suppose  $R = \mathbb{Z}/p(x)$ . Then  $R$  is a field. Consider the element  $x \in R$ . If  $x = F(a) = a^p$  for some  $a \in R$ , then  $a = \frac{f(x)}{g(x)}$  for  $f(x), g(x) \in \mathbb{Z}/p[x]$  and

$$x = \left( \frac{f(x)}{g(x)} \right)^p = \frac{(f(x))^p}{(g(x))^p},$$

so  $xg(x)^p = f(x)^p$ . If  $a_n x^n$  is the highest-order term of  $g(x)$  and  $b_m x^m$  is the highest-order term of  $f(x)$ , then this implies that

$$a_n x^{np+1} = b_m x^{mp},$$

so  $a_n = b_m$  and  $np + 1 = mp$ , which is clearly impossible, since  $p > 1$ . Therefore, we see that there is no element of  $R$  mapping to  $x$ , so  $F : R \rightarrow R$  is not surjective.



**(d):** If  $R$  is a finite field, show that  $F$  is an automorphism.

*Proof.* We showed, in (c), that  $F : R \rightarrow R$  is an injection. Since an injective map from a finite set to itself must be surjective, this suffices to show that  $F : R \rightarrow R$  is a bijection. Since  $F$  is also an endomorphism, this implies that  $F$  is an automorphism.  $\square$

Let  $K$  be a field and let  $G$  be a subgroup of the multiplicative group  $K^* = K - \{0\}$ .

**(a):** Show that if  $a, b \in K$  have finite orders  $m, n$ , then there is a  $c \in K$  whose order is the least common multiple of  $m, n$ .

*Proof.* First, suppose  $m$  and  $n$  are relatively prime. Then the l.c.m. of  $m$  and  $n$  is  $mn$ . Now, consider  $ab$ . First, note that

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n (b^n)^m = 1.$$

Furthermore, if  $1 = (ab)^k = a^k b^k$ , then  $b^k = (a^k)^{-1} = a^{-k}$ . Since the order of  $a^{-k}$  divides  $m$  and the order of  $b^k$  divides  $n$  and  $m$  and  $n$  are relatively prime, we see that  $b^k = a^{-k}$  has order 1; i.e.

$$a^{-k} = b^k = 1.$$

Hence,  $k$  is a multiple of both  $m$  and  $n$ , and so  $k$  is a multiple of  $mn$ . Therefore, we see that the order of  $ab$  is  $mn$ , the l.c.m. of  $m$  and  $n$ .

More generally, if  $a$  and  $b$  have orders  $m$  and  $n$ , respectively, let  $\ell$  be the l.c.m. of  $m$  and  $n$ . Then  $\ell = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  for  $p_i$  prime and  $\alpha_i \in \mathbb{N}$ . Now, if  $p_i^{\alpha_i} | m$ , then  $a^{m/(p_i^{\alpha_i})}$  has order  $p_i^{\alpha_i}$ ; similarly, if  $p_i^{\alpha_i} | n$ , then  $a^{n/(p_i^{\alpha_i})}$  has order  $p_i^{\alpha_i}$ . Hence, for each  $i$ , there exists  $c_i \in K$  such that  $c_i$  has order  $p_i^{\alpha_i}$ . Let

$$c = \prod_{i=1}^k c_i.$$

Then, since  $p_i^{\alpha_i}$  and  $p_j^{\alpha_j}$  are relatively prime for all  $i \neq j$ , the result proved above demonstrates that  $c$  has order

$$\prod_{i=1}^k p_i^{\alpha_i} = \ell.$$

□

**(b):** Show that if  $G$  is finite then it is cyclic.

*Proof.* Let  $\ell =$  the l.c.m. of the orders of the elements of  $G$ . Then  $\#(G)$  is a multiple of  $\ell$ . By 3(b), there are at most  $\ell$  roots of the polynomial  $x^\ell - 1$  in  $K$ . On the other hand, if  $a \in G$ , then  $a^\ell = 1$  since  $\ell$  is a multiple of the order of  $a$ . Hence, each element of  $G$  is a root of  $x^\ell - 1$ , so  $\#(G) = \ell$  and the elements of  $G$  are all the roots of  $x^\ell - 1$ . Now, by part (a), there exists  $c \in K$  such that the order of  $c$  is  $\ell$ . Since  $c$  is, thereby, a root of  $x^\ell - 1$ ,  $c \in G$ . Since all the powers of  $c$  are also solutions of  $x^\ell - 1$ , the  $\ell$  distinct powers of  $c$  are precisely the elements of  $G$ , so we see that  $G = \langle c \rangle$  is cyclic. □

(c): Conclude that if  $K \subset L$  is an extension of finite fields, then  $L = K[a]$  for some  $a \in K$ .

*Proof.* Since  $L$  is finite,  $L^*$  is also finite and so, by part (b) above,  $L^*$  is cyclic. Let  $a \in L^*$  be a generator of  $L^*$ ; then  $L = K[a]$ .  $\square$

DRL 3E3A, UNIVERSITY OF PENNSYLVANIA  
*E-mail address:* shonkwil@math.upenn.edu