Homework

Frederick Robinson

25 January 2010

Contents

1 Chapter 7 Section 3

1.1 Problem 13

1.1.1 Question

Prove that the ring $M_2(\mathbb{R})$ contains a subring that is isomorphic to $\mathbb{C}$.

1.1.2 Answer

I claim that the subring of $M_2(\mathbb{R})$ defined by

$$X = \left\{ \begin{bmatrix} r\cos\theta & -r\sin\theta \\ r\sin\theta & r\cos\theta \end{bmatrix} \mid r \in \mathbb{R}^+, \theta \in [0, 2\pi) \right\} \cap \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

is isomorphic to $\mathbb{C}$ via the isomorphism $\varphi : M_2(\mathbb{R}) \to \mathbb{C}$ defined as

$$\varphi\left(\begin{bmatrix} r\cos\theta & -r\sin\theta \\ r\sin\theta & r\cos\theta \end{bmatrix}\right) = re^{i\theta} \quad \varphi\left(\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\right) = 0$$

First we will prove that this is a homomorphism.

Proof. We need to show that $\varphi(a)+\varphi(b) = \varphi(a+b)$ and $\varphi(a)\cdot\varphi(b) = \varphi(a\cdot b)$

Assume without loss of generality that $a = 0$. Then, $\varphi(a) + \varphi(b) = \varphi(0) + \varphi(b) = \varphi(b) = \varphi(0 + b) = \varphi(a + b)$ and similarly $\varphi(a) \cdot \varphi(b) = \varphi(0) \cdot \varphi(b) = 0 \cdot \varphi(b) = 0 = \varphi(0) = \varphi(0 \cdot b)$. Hence we may assume that $a \neq 0, b \neq 0$.

Let

$$a = \begin{bmatrix} r\cos\theta & -r\sin\theta \\ r\sin\theta & r\cos\theta \end{bmatrix} \qquad b = \begin{bmatrix} d\cos\gamma & -d\sin\gamma \\ d\sin\gamma & d\cos\gamma \end{bmatrix}$$

So we have

$$\varphi(a{\cdot}b) = \varphi\left(\begin{bmatrix} dr\cos\gamma\cos\theta - dr\sin\gamma\sin\theta & -dr\cos\theta\sin\gamma - dr\cos\gamma\sin\theta \\ dr\cos\theta\sin\gamma + dr\cos\gamma\sin\theta & dr\cos\gamma\cos\theta - dr\sin\gamma\sin\theta \end{bmatrix}\right)$$

$$= \varphi\left(\begin{bmatrix} dr\left(\cos\gamma\cos\theta - \sin\gamma\sin\theta\right) & -dr\left(\cos\theta\sin\gamma + \cos\gamma\sin\theta\right) \\ dr\left(\cos\theta\sin\gamma + \cos\gamma\sin\theta\right) & dr\left(\cos\gamma\cos\theta - \sin\gamma\sin\theta\right) \end{bmatrix}\right)$$

Now recall the trigonometric identities $\sin(\alpha+\beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta$ and $\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$. Employing these we rewrite the forgoing as

$$\varphi\left(\begin{bmatrix} dr\cos(\theta+\gamma) & -dr\sin(\theta+\gamma) \\ dr\sin(\theta+\gamma) & dr\cos(\theta+\gamma) \end{bmatrix}\right) = (dr)e^{i(\theta+\gamma)} = \left(de^{i\theta}\right)\cdot\left(re^{i\gamma}\right)$$

$$= \varphi\left(\begin{bmatrix} r\cos\theta & -r\sin\theta \\ r\sin\theta & r\cos\theta \end{bmatrix}\right)\cdot\varphi\left(\begin{bmatrix} d\cos\gamma & -d\sin\gamma \\ d\sin\gamma & d\cos\gamma \end{bmatrix}\right) = \varphi(a)\cdot\varphi(b)$$

Moreover we observe that

$$\varphi(a) + \varphi(b) = re^{i\theta} + de^{i\gamma} = r\left(\cos\theta + i\sin\theta\right) + d\left(\cos\gamma + i\sin\gamma\right)$$

$$= \left(r\cos\theta + d\cos\gamma\right) + i\left(r\sin\theta + d\sin\gamma\right)$$

$$= \varphi\left(\begin{bmatrix} (r\cos\theta + d\cos\gamma) & -(r\sin\theta + d\sin\gamma) \\ (r\sin\theta + d\sin\gamma) & (r\cos\theta + d\cos\gamma) \end{bmatrix}\right) = \varphi(a+b)$$

So we have verified that φ is a ring homomorphism as desired □

Now that we have established that φ is a homomorphism we need to show that it is bijective. However, this just follows from the uniqueness of the polar representation of complex numbers.

Since each complex number can be expressed uniquely in the form $w = re^{i\theta}$ with $\theta \in [0, 2\pi)$ it must be that the homomorphism defined above is surjective. Moreover, it must be injective since, if there were two a, b with $a \neq b$ such that $\varphi(a) \neq \varphi(b)$ this would mean that the polar representation of complex numbers is not unique.

Note that although I did not show explicitly that X is a subring of $M_2(\mathbb{R})$ this must be the case, since it is related by a bijective homomorphism to $\mathbb{C}$ which we know to be a ring. This implies that it is closed under inverses (the inverse of $a \in X$ is just $\varphi^{-1}(\varphi(a)^{-1})$) and closed under the ring operations (in particular we have $\varphi^{-1}(\varphi(a) + \varphi(b)) = a + b$ and $\varphi^{-1}(\varphi(a) \cdot \varphi(b)) = a \cdot b$)

1.2 Problem 16

1.2.1 Question

Let $\varphi : R \to S$ be a surjective homomorphism of rings. Prove that the image of the center or R is contained in the center of S (cf. Exercise 7 of Section 11).

1.2.2 Answer

Let $r \in R$ be a member of the center of a ring R. I claim that if $\varphi : R \to S$ is a surjective ring homomorphism then $\varphi(r) \in Z_S$ where Z_S is the center of the ring S.

Proof. Let $s \in S$ be a member of the ring S. Since φ is surjective we may write s as $s = \varphi(x)$ for some $x \in R$. Thus, for r an element of the center of R we have $\varphi(r)s = \varphi(r)\varphi(x) = \varphi(rx) = \varphi(xr) = \varphi(x)\varphi(r) = s\varphi(r)$. Since s was chosen arbitrarily it must be that $\varphi(r)$ commutes with any element of S and is therefore a member of the center of S.

Moreover, we have that each element of the center of R is mapped by φ to a member of the center of S, and the image of the center of R is contained in the center of S as desired. □

1.3 Problem 17

1.3.1 Question

Let R and S be nonzero rings with identity and denote their respective identities by 1_R and 1_S. Let $\varphi : R \to S$ be a nonzero homomorphism of rings.

1. Prove that if $\varphi(1_R) \neq 1_S$ then $\varphi(1_R)$ is a zero divisor in S. Deduce that if S is an integral domain then every ring homomorphism from R to S sends the identity of R to the identity of S.

2. Prove that if $\varphi(1_R) = 1_S$ then $\varphi(u)$ is a unit in S and that $\varphi(u^{-1}) = \varphi(u)^{-1}$ for each unit u of R.

1.3.2 Answer

Let R and S be nonzero rings with identity and $\varphi : R \to S$ be a nonzero ring homomorphism.

1. If $\varphi(1_R) \neq 1_S$ then $\varphi(1_R)$ is a zero divisor in S.

   Proof. Assume $\varphi(1_R) \neq 1_S$

   We have $\varphi(1_R) \cdot \varphi(1_R) = \varphi(1_R \cdot 1_R) = \varphi(1_R) \Rightarrow \varphi(1_R)\,(\varphi(1_R) - 1_S) = 0$ however since we have also that φ is a nonzero homomorphism and $\varphi(1_R) \neq 1_S$ it must be that $\varphi(1_R) \neq 0$ is a zero divisor. □

   This established it is clear that if S is an integral domain $\varphi(1_R) = 1_S$ since there are no zero divisors in integral domains, and integral domains.

2. Let $\varphi(1_R) = 1_S$ then for u a unit in R we have $\varphi(uu^{-1}) = \varphi(1_R) = 1_S = \varphi(u)\varphi(u^{-1})$ so $\varphi(u)$ is a unit in S with inverse $\varphi(u^{-1})$.

1.4 Problem 19

1.4.1 Question

Prove that if $I_1 \subseteq I_2 \subseteq \cdots$ are ideals of R then $\cup_{n=1}^{\infty} I_n$ is an ideal of R.

1.4.2 Answer

Let $i \in \cup_{n=1}^{\infty} I_n$. I claim that $ix = j$ for each $x \in R$ some $j \in \cup_{n=1}^{\infty} I_n$

Proof. In particular we must have some k such that $i \in I_m$ for all $m \geq k$. So, since I_k is an ideal it must be that $ix = j$ for each $x \in R$ some $j \in I_k$. Since $I_k \subseteq \cup_{n=1}^{\infty} I_n$ we have moreover that $ix = j$ for each $x \in R$ some $j \in \cup_{n=1}^{\infty} I_n$ as claimed. □

So $\cup_{n=1}^{\infty} I_n$ is an idea of R as desired.

1.5 Problem 26

1.5.1 Question

The *characteristic* of a ring R is the smallest positive integer n such that $1 + 1 + \cdots + 1 = 0$ (n times) in R; if no such integer exists the characteristic or R is said to be 0. For example, $\mathbb{Z}/n\mathbb{Z}$ is a ring of characteristic n for each positive integer n and $\mathbb{Z}$ is a ring of characterisitic 0.

1. Prove that the map $\mathbb{Z} \to R$ defined by

$$k \mapsto \begin{cases} 1 + 1 + \cdots + 1 \text{ (k times)} & \text{if } k > 0 \\ 0 & \text{if } k = 0 \\ -1 - 1 - \cdots - 1 \text{ ($-k$ times)} & \text{if } k < 0 \end{cases}$$

is a ring homomorphism whose kernel is $n\mathbb{Z}$, where n is the characteristic of R (this explains the use of the terminology "characteristic 0" instead of the archaic phrase "characteristic ∞" for rings in which no sum of 1's is zero).

2. Determine the characteristic of the rings $\mathbb{Q}$, $\mathbb{Z}[x]$, $\mathbb{Z}/n\mathbb{Z}[x]$.

3. Prove that if p is prime and if R is a commutative ring of characteristic p, then $(a+b)^p = a^p + b^p$ for all $a, b \in R$.

1.5.2 Answer

1. The above defined map is a homomorphism.

Proof. If one of a or b (say without loss of generality a) is zero then we have that $\varphi(0)+\varphi(b) = 0 + \underbrace{1+1+\cdots+1}_{b \text{ times}} = \varphi(b)$ or $\varphi(0)+\varphi(b) = 0 + \underbrace{-1-1-\cdots-1}_{|b| \text{ times}} = \varphi(b)$

Similarly with multiplication we get $\varphi(0)\cdot\varphi(b) = 0\cdot\varphi(b) = 0 = \varphi(0\cdot b)$

There remain only three cases.

Case 1: a and b are both positive. $\varphi(a)+\varphi(b) = \underbrace{1+1+\cdots+1}_{\text{a times}} + \underbrace{1+1+\cdots+1}_{\text{b times}} = \underbrace{1+1+\cdots+1}_{\text{a+b times}} = \varphi(a+b)$.

Similarly we observe that $\varphi(a)\cdot\varphi(b) = \underbrace{(1+1+\cdots+1)}_{\text{a times}}\cdot\underbrace{(1+1+\cdots+1)}_{\text{b times}}$ and exploiting distributivity this is just $\underbrace{(1+1+\cdots+1)}_{a\cdot b \text{ times}} = \varphi(a\cdot b)$

Case 2: a and b are both negative. $\varphi(a)+\varphi(b) = \underbrace{-1-1-\cdots-1}_{\text{|a| times}} + \underbrace{-1-1-\cdots-1}_{\text{|b| times}} = \underbrace{-1-1-\cdots-1}_{\text{|a+b| times}} = \varphi(a+b)$

Similarly we observe that $\varphi(a)\cdot\varphi(b) = \underbrace{(-1-1-\cdots-1)}_{\text{|a| times}} \cdot \underbrace{(-1-1-\cdots-1)}_{\text{|b| times}}$ and exploiting distributivity this is just $\underbrace{(1+1+\cdots+1)}_{a\cdot b \text{ times}} = \varphi(a\cdot b)$

Case 3: WLOG a is positive and b negative. $\varphi(a)+\varphi(b) = \underbrace{1+1+\cdots+1}_{\text{a times}} + \underbrace{-1-1-\cdots-1}_{\text{|b| times}} =$

Case i: $(|b| < |a|)$ $\underbrace{1+1+\cdots+1}_{\text{a+b times}} = \varphi(a+b)$

We have also that $\varphi(a)\cdot\varphi(b) = \underbrace{(1+1+\cdots+1)}_{\text{|a| times}} \cdot \underbrace{(-1-1-\cdots-1)}_{\text{|b| times}}$ and exploiting distributivity this is just $\underbrace{(-1-1-\cdots-1)}_{|a\cdot b| \text{ times}} = \varphi(a\cdot b)$

Case ii: $(|b| > |a|)$ $\underbrace{-1-1-\cdots-1}_{\text{|a+b| times}} = \varphi(a+b)$.

We have also that $\varphi(a)\cdot\varphi(b) = \underbrace{(1+1+\cdots+1)}_{\text{|a| times}} \cdot \underbrace{(-1-1-\cdots-1)}_{\text{|b| times}}$ and exploiting distributivity this is just $\underbrace{(-1-1-\cdots-1)}_{|a\cdot b| \text{ times}} = \varphi(a\cdot b)$ □

The kernel of this homomorphism is all integers of the form $n\mathbb{Z}$ where n is the characteristic of R since $z \in \mathbb{Z}$ is a member of the kernel if and only if $\varphi(z) = 0$.

0 is always in the kernel by definition of φ.

Moreover, the least positive element of $\mathbb{Z}$ which is mapped to 0 is n since the characteristic of a ring is precisely the least n such that $\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$. So each element of form $n\mathbb{Z}$ must also be mapped to 0 in R since we can write such an element as $m \cdot n$ and by homomorphism property we have $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) = \varphi(m) \cdot 0 = 0$. Lastly an element not of this form may not map to 0 since we may write such an element as $m \cdot n + r$ with $r < n$ by the Euclidean Domain property. So, applying the transformation and using properties of homomorphisms we have $\varphi(m \cdot n + r) = \varphi(m) \cdot \varphi(n) + \varphi(r) = 0 + \varphi(r) = \varphi(r)$ and we know that $\varphi(r) \neq 0$ since by the previous n is the least element of $\mathbb{Z}$ such that $\varphi(n) = 0$.

It remains only to show that if R is a ring of characteristic 0 then the only element of $\mathbb{Z}$ which maps to the 0 element of R is the 0 element in $\mathbb{Z}$. We have shown already that 0 must be a member of the kernel. If there were some nonzero element in the kernel then it would follow that $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$ or $\underbrace{-1 - 1 - \cdots - 1}_{n \text{ times}} = 0$ but this is contradictory to the definition of having characteristic 0.

2. The ring $\mathbb{Q}$ has characteristic 0 since $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = n \neq 0$ for all $n \in \mathbb{N}$

   The ring $\mathbb{Z}[x]$ has characteristic 0 since $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = n \neq 0$ for all $n \in \mathbb{N}$

   The ring $\mathbb{Z}/n\mathbb{Z}[x]$ has characteristic n since $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$ for n and moreover $\underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} \neq 0$ for $m < n$. This follows from the fact that the integers mod n have characteristic n.

3. If p is prime and if R is a commutative ring of characteristic p, then $(a+b)^p = a^p + b^p$ for all $a, b \in R$.

   Proof. Since R is a commutative ring we know by the binomial expansion that the coefficient of the a^kth term is given by

   $$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

   Since p is prime this number is a multiple of p and therefore the coefficient is just 0, except of course in the case where $k = 0$ or $k = p$.

   This is just what we wanted to prove though as it means that we may write the product as $a^p + b^p$ □

1.6 Problem 28

1.6.1 Question

Prove that an integral domain has characteristic p, p is either prime or 0 (cf. Exercise 26).

1.6.2 Answer

An integral domain is a commutative ring with $1 \neq 0$ and with no zero divisors. We will demonstrate first that an integral domain can exist with characteristic either 0 or p, and then that no integral domain with a different characteristic can exist.

Proof. An example of an integral domain with characteristic 0 is the set $\mathbb{Z}$ of all real numbers. We have demonstrated before that this is an integral domain. Also, the field $\mathbb{F}_p$ with p prime is in particular an integral domain.

Since we have demonstrated that there are integral domains with characteristic p and 0 all we need to do now is prove that there can exist no integral domain with characteristic $n \neq 0$ n prime.

So, suppose towards a contradiction that there does exist an integral domain of characteristic n as defined above. This means that $\underbrace{1 + 1 + \cdots 1}_{n \text{ times}} = 0$ and moreover that n is the least number such that this is true.

However since n is composite there must be some m and l neither 1 such that $l \cdot m = n$ and $m < n$, $l < n$. However, this implies that $\underbrace{(1 + 1 + \cdots 1)}_{l \text{ times}} \cdot \underbrace{(1 + 1 + \cdots 1)}_{m \text{ times}} = \underbrace{1 + 1 + \cdots 1}_{l \cdot m \text{ times}} = 0$. Since l and m are both less than n neither of the sums in the above product may be zero. Hence, they are zero divisors. Contradiction. □

2 Chapter 7 Section 4

2.1 Problem 4

2.1.1 Question

Assume R is commutative. Prove that R is a field if and only if 0 is a maximal ideal.

2.1.2 Answer

We prove first (⇒) that R a field implies that 0 is a maximal ideal. Let R be a field. We prove that 0 is a maximal ideal.

Proof. Since 0 is contained in every ideal saying that 0 is a maximal ideal is equivalent to saying that the only ideals are 0 and R. If I is an ideal in R and $i \in I$ is a nonzero element of the ideal then it must be that $I = R$ since, because R is a field every element of R is a unit. In particular i is a unit. Thus $i^{-1} \in I \Rightarrow 1 \in I \Rightarrow R = I$. Since we have established that every nonzero ideal of R is R itself it must be that R and 0 are the only ideals of R and in particular 0 is a maximal ideal of R □

Now we prove (⇐) that if 0 is a maximal ideal then R is a field. Assume that 0 is a maximal ideal.

Proof. Since 0 is a maximal idea it must be that the only ideals of R are 0 and R itself. For, 0 is contained in every ideal, and so if there were some ideal in R that was not R or 0, 0 would not be maximal. This established suppose towards a contradiction that R is not a field. This implies in particular that there is some element $i \in R$ that has no inverse, as R is an integral domain. Take then (i) the ideal generated by i. This is an ideal of R by definition, and moreover we know that it may not contain the element 1 since i has no inverse and $(i) = \{r \cdot i \mid r \in R\}$. If this ideal were to contain 1 it would imply that i had an inverse. We have however just constructed an ideal of R which is not 0 or R. Contradiction. □

2.2 Problem 8

2.2.1 Question

Let R be an integral domain. Prove that $(a) = (b)$ for some elements $a, b \in R$, if and only if $a = ub$ for some unit u of R.

2.2.2 Answer

We prove first ($\Rightarrow$) that if $(a) = (b)$ for some $a, b \in R$ an integral domain then $a = ub$ for some unit u.

Proof. Assume that $(a) = (b)$, then it must be that $(a) = \{ar \mid r \in R\} = \{br \mid r \in R\} = (b)$. In particular we must have that for each $r \in R$ there exists some other $r' \in R$ such that $ar = br'$. Since R is an integral domain we have $1 \in R$ and commutativity so we may say $\exists r'$ such that $a1 = a = br' = r'b$. Similarly there must exist r such that $ra = b$. Taken together these statements imply that $r'(ra) = a \Rightarrow (r'r)a = a$ so r and r' are units. Thus, there must exist a unit such that $a = r'b$ as claimed. □

Conversely we claim that if there exists a unit u such that $a = ub$ then $(a) = (b)$

Proof. We show first that $(b) \subseteq (a)$. Since u is a unit we have $b = u^{-1}a$ and the same argument shows $(a) \subseteq (b) \Rightarrow (a) = (b)$.

Let $x \in (b)$. So we may write $x = rb$ for some $r \in R$ We must also have $x \in (a)$ since u is a unit, which implies that $rb = ru^{-1}ub = ru^{-1}a$. So there exists $x' = ru^{-1} \in R$ such that $x'a = xb$ for each xb in (b). Thus $(b) \subseteq (a)$ as claimed. □

2.3 Problem 15

2.3.1 Question

Let $x^2 + x + 1$ be an element of the polynomial ring $E = \mathbb{F}_2[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{F}_2[x]/(x^2 + x + 1)$.

1. Prove that $\bar{E}$ has 4 elements: $\bar{0}, \bar{1}, \bar{x}$ and $\overline{x+1}$.
2. Write out the 4×4 addition table for $\overline{E}$ and deduce that the additive group $\overline{E}$ is isomorphic to the Klein 4-group.
3. Write out the 4×4 multiplication table for $\overline{E}$ and prove that $\overline{E}^{\times}$ is isomorphic to the cyclic group of order 3. Deduce that $\overline{E}$ is a field.

2.3.2 Answer

1. First we will demonstrate a process by which given a polynomial of a degree greater than two we can produce a representative of the same equivalence class mod $x^2 + x + 1$ with degree less than two.

   First, note that the ideal $(x^2 + x + 1)$ contains elements with of degree n for any $n \geq 2$. In particular we may construct such an element as $x^{n-2}(x^2 + x + 1)$.

Now, given an arbitrary member of $\mathbb{F}_2[x]$ say g we may produce a member of the same equivalence class as g but with degree less than two by adding a member of the ideal $(x^2 + x + 1)$ to the polynomial repeatedly.

Since adding a member of the ideal to our polynomial preserves the equivalence class we can do this as many times as desired. Moreover, since in $\mathbb{F}$ $1 + 1 = 0$ and a polynomial must have coefficient 1 corresponding to its order we always decrease the order of g by adding an element of $(x^2 + x + 1)$ with the same order as g.

We have shown already that we can construct such elements of $(x^2 + x + 1)$ so we are done.

So, since given a polynomial we can construct a member of the same equivalence class with order less than two there may be at most one equivalence class for each such polynomial. That is, the only candidates for equivalence classes are:

$\overline{1}, \overline{0}, \overline{x}, \overline{x+1}$

Now suppose towards a contradiction that one of these equivalence classes was the same as one of the other equivalence classes. This would mean in particular that given one of the representatives above say f there is another representative in the above list, say g such that $f + i = g$ for some element i of the ideal $(x^2 + x + 1)$ generated by $x^2 + x + 1$.

However each of the elements in the above list has order less than 2, and each element $i \in (x^2+x+1)$ has order at least 2. For, suppose not, then there exists some polynomial $h \in \mathbb{F}_2[x]$ such that $h(x^2+x+1)$ has order less than two. Since the coefficient of the maximal component of a product is the product of the coefficients of the maximal components in each polynomial in that product we must have $h = 0$. However, this implies that $h(x^2 + x + 1) = 0$

So, we may not write $f + i = g$ for $i \in (x^2 + x + 1)$, and each of the equivalence classes $\overline{0}, \overline{1}, \overline{x}, \overline{x+1}$ are unique.

So, $E = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$ as desired.

2.

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

This is isomorphic to the Klein 4-group by inspection (compare with the table on page 68)

3.

$\times$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

$E^\times$ is isomorphic to the cyclic group of order 3 by the following isomorphism. $\overline{1} = 0$, $\overline{x+1} = 1$, $\overline{x} = 2$. Since the addition table for the cyclic group of order 3 is

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cong$

$+$	$\overline{1}$	$\overline{x+1}$	$\overline{x}$
$\overline{1}$	$\overline{1}$	$\overline{x+1}$	$\overline{x}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$
$\overline{x}$	$\overline{x}$	$\overline{1}$	$\overline{x+1}$

Finally we recognize that E must be a field since $E^\times$ is isomorphic to the cyclic group which is a group, and therefore has identity, inverse. Also the cyclic group is commutative.