

MATH 74, FALL 2004, HOMEWORK 11 SOLUTIONS

BENJAMIN JOHNSON

Due November 17

Assignment: 3.1.3, 3.1.22, 3.1.23(1)(2b)(3), 3.2.2(b)

3.1.3 Is each of the following a field? Why or why not?

- (a) \mathbb{R}^+ is **not a field** because, for example, $1 \in \mathbb{R}^+$, but 1 does not have an additive inverse in \mathbb{R}^+ , in violation of axiom (A3) for fields. For proof that 1 does not have an additive inverse, we notice that for any element of $a \in \mathbb{R}^+$, $a \cdot 1 > 0 \neq 0$.
- (b) \mathbb{R}^2 with addition and multiplication defined by $(x, y) + (u, v) = (x + u, y + v)$ and $(x, y) \cdot (u, v) = (x \cdot u, y \cdot v)$ is **not a field**, because, for example, $(0, 1)$ is a non-zero element of \mathbb{R}^2 that does not have a multiplicative inverse, in violation of axiom (M3) for fields. It is easy to show that the additive identity of \mathbb{R}^2 (with $+$ and \cdot defined as above) is $(0, 0)$ and that the multiplicative identity is $(1, 1)$. Now for any $(a, b) \in \mathbb{R}^2$, we have $(a, b) \cdot (0, 1) = (0, b) \neq (1, 1)$ (regardless of our choice of a and b). This proves that $(0, 1)$ has no multiplicative inverse in \mathbb{R}^2 .
- (c) The set F consisting of all integers together with the reciprocals of all integers added and multiplied in the usual way is **not a field** because it is not closed under addition. This violates our assumption about the structure of F that says $+$ is a binary operation on F . For example, $\frac{1}{2}, \frac{1}{3} \in F$, but $\frac{1}{2} + \frac{1}{3} = \frac{5}{6} \notin F$.
- (d) $\mathbb{Q}(\sqrt{2})$ is **a field**. Since $\mathbb{Q}(\sqrt{2})$ is clearly a subset of the field \mathbb{R} , we only need to verify that this set is closed under all of the field operations $+\mathbb{R}$, $\cdot\mathbb{R}$, $-\mathbb{R}$, $^{-1}\mathbb{R}$, $0\mathbb{R}$, and $1\mathbb{R}$. $\mathbb{Q}(\sqrt{2})$ is closed under addition and multiplication since for any $a, b, c, d \in \mathbb{Q}$, $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. It is closed under additive inverses since for any $a, b \in \mathbb{Q}$, the additive inverse of $a + b\sqrt{2}$ is $(-a) + (-b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. It is closed under multiplicative inverses since for any $a, b \in \mathbb{Q}$, the multiplicative inverse of $a + b\sqrt{2}$ is $\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 + 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Both $0_{\mathbb{R}} = 0 + 0\sqrt{2}$ and $1_{\mathbb{R}} = 1 + 0\sqrt{2}$ are in $\mathbb{Q}(\sqrt{2})$. So $\mathbb{Q}(\sqrt{2})$ is closed under all the field operations of \mathbb{R} , and is hence a field.
- (e) The set \mathcal{P} of all polynomial functions $p : \mathbb{R} \rightarrow \mathbb{R}$ is **not a field**, because, for example, the element $x \in \mathcal{P}$ does not have a multiplicative inverse in \mathcal{P} , in violation of axiom (M3) for fields. It is easy to show that the additive identity element for \mathcal{P} is the constant zero polynomial and that the multiplicative identity for \mathcal{P} is the constant one polynomial (i.e, the polynomial $p(x) = 1$). Now the zero polynomial is not a multiplicative inverse for x . If $p(x)$ is any non-zero element of \mathcal{P} , then the degree of $p(x) \cdot x$ must be at least 1, and hence cannot be the constant one polynomial, which has degree zero. This shows that x has no multiplicative inverse in \mathcal{P} .

3.1.22 Show that every finite field has characteristic $n > 0$.

Proof. Let F be a finite field, and suppose F has k elements. We know that for each $n \in \mathbb{N}$, $n_F = 1_F + \cdots + 1_F$ (n -times) is an element of F . By the pigeon-hole principle, the $k + 1$ elements $0_F, \dots, k_F$ cannot all be distinct. So there must exist $r, s \in \mathbb{N}$ with $0 \leq r < s \leq k$

and $r_F = s_F$. Now $s - r \in \mathbb{N}^*$ since $s > r$. Furthermore $(s - r)_F = s_F + (-r_F) = r_F + -r_F = 0_F$. So $(\exists n \in \mathbb{N}^*)(n_F = 0_F)$. Thus F has finite characteristic $n > 0$. \square

Side note: The pigeonhole principle says that if $n > k$, and we cram n pigeons into k pigeonholes, at least one hole will have more than one pigeon in it.

3.1.23(1) Prove that if a field F has characteristic $n > 0$, then n must be a prime number.

Proof. We'll use proof by contradiction. Suppose F has characteristic $n > 0$ (so that n is the least positive integer with $n_F = 0_F$) and that n is not a prime number. We cannot have $n = 1$, because this would imply $1_F = 0_F$ in contradiction to the field axiom (M2). Since n is not prime and $n > 1$, n must be composite, and so there are integers $a, b \in \mathbb{N}$ with $2 \leq a, b < n$ and $n = ab$. Now a_F, b_F, n_F are all elements of F and $a_F \cdot b_F = n_F = 0_F$. There are several ways to show that this scenario leads to a contradiction. One way is the following: $b_F = 1_F \cdot b_F = (a_F^{-1} \cdot a_F) \cdot b_F = a_F^{-1} \cdot (a_F \cdot b_F) = a_F^{-1} \cdot n_F = a_F^{-1} \cdot 0_F = 0_F$. So $b_F = 0_F$. Since $b \in \mathbb{N}^*$ and $b < n$, this contradicts our assumption that n was the least positive integer with $n_F = 0$.

Notice that we did not need the assumption (stated in the textbook) that F was a finite field in order to obtain the contradiction. So if F is any field with finite characteristic $n > 0$, n must be a prime number. \square

3.1.23(2b) Given the following addition and multiplication tables for a set $F = \{0, 1, \alpha, \beta\}$:

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Assuming that these operations satisfy the field axioms, determine the characteristic of F .

The characteristic of F is 2 because $2_F = 1_F + 1_F = 0$ and 2 is the least positive integer with $2_F = 0_F$.

3.1.23(3) If F is a finite field, prove that the characteristic p of F must divide the number of elements of F .

Proof. Let F be a finite field with characteristic p . We need to show that p divides the number of elements of F . To do this, we will show that F can be partitioned into some number of disjoint subsets (equivalence classes), each of which has exactly p elements. If there are k such subsets, then the number of elements in F will be $k \cdot p$, so that p divides the number of elements of F . Elements of F will be in the same subset (equivalence class) if they differ from one another by some n_F with $n \in \mathbb{Z}$. The formal proof follows.

Define a two-place relation \sim on F via, for $a, b \in F$, $a \sim b$ iff $(\exists n \in \mathbb{Z})(b = a + n_F)$. I claim that \sim is an equivalence relation on F .

- (1) \sim is reflexive since for $a \in F$, $a + 0_F = a$, and so $a \sim a$.
- (2) \sim is symmetric since for $a, b \in F$, if $a \sim b$, then $(\exists n \in \mathbb{Z})(b = a + n_F)$. It is easy to show $a = b + (-n)_F$, so that $b \sim a$.
- (3) \sim is transitive since for $a, b, c \in F$, if $a \sim b$ and $b \sim c$, then $(\exists n, m \in \mathbb{Z})(b = a + n_F \wedge c = b + m_F)$, and so $c = a + (n + m)_F$, so that $a \sim c$.

This proves the claim.

For $a \in F$, define $[a]_{\sim} = \{b \in F : a \sim b\}$. $[a]_{\sim}$ is the equivalence class of a under the equivalence relation \sim . Straight from the definitions we have $[a]_{\sim} = \{a + n_F : n \in \mathbb{Z}\}$, but because F has finite characteristic, many of the n_F 's listed here represent the same field element. In fact, I claim that the set $\{n_F : n \in \mathbb{Z}\}$ is really just the p -element set $\{0_F, \dots, (p-1)_F\}$.

- (1) $\{n_F : n \in \mathbb{Z}\}$ has at most p elements. This is because $p_F = 0_F$ and so for any integer k , $k = (k \operatorname{div} p) \cdot p + (k \bmod p)$, and so $k_F = 0_F + (k \bmod p)_F = (k \bmod p)_F$, and $(k \bmod p)$ is an integer between 0 and $p-1$.
- (2) $\{n_F : n \in \mathbb{Z}\}$ has at least p elements. This is because the elements $\{0_F, \dots, (p-1)_F\}$ are all distinct. As we saw in the proof of 3.1.22, we obtain a contradiction if we assume that there exist r, s with $0 \leq r < s \leq p-1$ and $r_F = s_F$.

This proves the claim.

So $[a]_{\sim} = \{a + n_F : 0 \leq n \leq p-1\}$. The p elements listed for $[a]_{\sim}$ must all be distinct, since if $a + n_F = a + m_F$, adding $-a$ to each side of the equation yields an immediate contradiction to the previous claim. So $[a]_{\sim}$ has exactly p elements, and since a was an arbitrary element of F , the same result holds for the equivalence class of every other element of F . Since any pair of equivalence classes is either disjoint or equal, we see that F can be partitioned into its various equivalence classes, (say there are k of them), each of which has exactly p elements. So the number of elements of F is exactly $k \cdot p$ and hence p divides the number of elements of F . □

3.2.2(b) For $\langle F, P \rangle$ an ordered field, show that $1_F \in P$.

Proof. The axiom (M2) for fields tells us that $1_F \neq 0_F$. So by the axiom (O1) for ordered fields, we know that exactly one of $1_F \in P$ or $-1_F \in P$ holds. It only remains to show that the latter case cannot be true. To obtain a contradiction, suppose $-1_F \in P$. Then by (O3), $-1_F \cdot -1_F \in P$. But by proposition 3.1.12(6), $-1_F \cdot -1_F = 1_F \cdot 1_F$ and $1_F \cdot 1_F = 1_F$ (by (M2)). So $1_F \in P$. This contradicts (O1) since we were assuming $-1_F \in P$. We conclude that $1_F \in P$. □