Jacobs University
School of Engineering and Science

Spring Term 2010

Linear Algebra II, Bonus homework

Introduction to fields

Due Date: Thursday, April 8, in class.

Definition. A *field* is a set $\mathbb{F}$ with two binary operations "+" and "·" on $\mathbb{F}$ called *addition* and *multiplication* satisfying the following properties:

1. $\forall a, b \in \mathbb{F} \quad a + b = b + a$;
2. $\forall a, b, c \in \mathbb{F} \quad (a + b) + c = a + (b + c)$;
3. there exists an element $0 \in \mathbb{F}$ such that $\forall a \in \mathbb{F} \quad a + 0 = a$;
4. $\forall a \in \mathbb{F}\, \exists b \in \mathbb{F} \quad a + b = 0$; b is called *opposite* to a and is denoted by $-a$;
5. $\forall a, b \in \mathbb{F} \quad (a \cdot b) = (b \cdot a)$;
6. $\forall a, b, c \in \mathbb{F} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$;
7. there exists an element $1 \in \mathbb{F}$ such that $\forall a \in \mathbb{F} \quad a \cdot 1 = a$, and $1 \neq 0$;
8. $\forall a \neq 0\, \exists b \in \mathbb{F} \quad a \cdot b = 1$; b is called *inverse* to a and is denoted by a^{-1} or $\frac{1}{a}$;
9. $\forall a, b, c \in \mathbb{F} \quad (a + b) \cdot c = a \cdot c + b \cdot c$.

B.1. Show that

(a) 0 is unique; 1 is unique;

(b) the opposite element is unique; the inverse element is unique;

(c) the equation $a + x = b$ has a unique solution in $\mathbb{F}$; the equation $a \cdot x = b$ has a unique solution in $\mathbb{F}$ for any $a \neq 0$;

(d) $a \cdot b = 0$ implies $a = 0$ or $b = 0$.

B.2. Show that the set $\{0, 1, \dots, p-1\}$ (p is prime) with operations of addition and multiplication modulo p is a field (notation: $\mathbb{Z}_p$ or $\mathbb{F}_p$).

Definition. $\mathbb{F}_0 \subset \mathbb{F}$ is a *subfield* of $\mathbb{F}$ if $\mathbb{F}_0$ is a field with respect to operations of $\mathbb{F}$.

B.3. (a) Define $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. Show that $\mathbb{Q}[\sqrt{2}]$ is a subfield of $\mathbb{R}$.

(b) Is the following set $\{a + b\sqrt{2} + c\sqrt{3} | a, b, c \in \mathbb{Q}\}$ a subfield of $\mathbb{R}$?

(c) Find all subfields of $\mathbb{Q}$, $\mathbb{Z}_p$, $\mathbb{Q}[\sqrt{2}]$.

Definition. A map $\psi : \mathbb{F} \to \mathbb{F}'$ is an *isomorphism of fields* $\mathbb{F}$ and $\mathbb{F}'$ if ψ is bijective, and $\forall a, b \in \mathbb{F} \quad \psi(ab) = \psi(a)\psi(b),\ \psi(a + b) = \psi(a) + \psi(b)$. Fields $\mathbb{F}$ and $\mathbb{F}'$are *isomorphic* if there exists an isomorphism from $\mathbb{F}$ to $\mathbb{F}'$.

B.4. (a) Isomorphism is equivalence relation.

(b) Every field has a subfield isomorphic either to $\mathbb{Q}$ or to $\mathbb{Z}_p$.

Definition. A field $\mathbb{F}$ has *characteristic* p (or 0) if it contains a subfield isomorphic to $\mathbb{Z}_p$ (respectively, $\mathbb{Q}$). Notation: $\operatorname{char}\mathbb{F} = p$ ($\operatorname{char}\mathbb{F} = 0$).

B.5. (a) Show that characteristic is well-defined.

(b) Which of the fields $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{R}$ are isomorphic?

B.6. (a) If $\mathbb{F}$ is finite and $\operatorname{char}\mathbb{F} = p$, then the map $x \to x^p$ is an automorphism of $\mathbb{F}$ (i.e. isomorphism onto itself).

(b) For $\mathbb{Z}_p$ the map $x \to x^p$ is an identity (Fermat Theorem).

B.7. (a) Show that there exists a unique (up to isomorphism) field consisting of 4 elements. What is the characteristic?

(b) Show that all fields consisting of p elements are isomorphic.

B.8. Is it true that the equation $x^2 = a$ for $a \neq 0$ has either 2 or 0 solutions?

B.9. Any finite field of characteristic p contains exactly p^n elements for some integer n.

B.10. For a field $\mathbb{F}$ and $c \in \mathbb{F}$ denote by $\mathbb{F}[\sqrt{c}]$ the set $\mathbb{F} \times \mathbb{F}$ with operations

1) $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$;

2) $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 + c b_1 b_2, a_1 b_2 + a_2 b_1)$.

For which c the set $\mathbb{F}[\sqrt{c}]$ will be a field if

(a) $\mathbb{F} = \mathbb{R}$; (b) $\mathbb{F} = \mathbb{Q}$; (c) $\mathbb{F} = \mathbb{Z}_p$, $p = 2, 3, 5, 7$?

B.11. For every odd prime p there exists c such that $\mathbb{F}[\sqrt{c}]$ is a field.

B.12. For any prime p

(a) there exists a field of p^2 elements;

(b) for any positive integer n there exists a field of p^n elements.