Some Useful Definitions

We summarize here a few of the definitions that will be used during the course.

Definition 1. A *group* G is a non-empty set, together with a single binary operation denoted here by $\star$

$$\begin{aligned} \star : G \times G &\longrightarrow G \\ (g,h) &\mapsto g \star h \end{aligned}$$

for all $g, h \in G$ such that the following axioms are satisfied:

1. Associativity:
$$g \star (h \star k) = (g \star h) \star k$$
for all $g, h, k \in G$;
2. An identity $e \in G$ exists:
$$e \star g = g \star e = g$$
for all $g \in G$;
3. Inverses exist:
For each $g \in G$ there exists an element $g' \in G$ such that
$$g \star g' = g' \star g = e$$

It is easy to check that

The identity is unique:
$$e = e \star e' = e'$$
for $e, e' \in G$ two possibly different identities satisfying 2. above.

Inverses are unique:
$$\begin{aligned} g'' \star (g \star g') &= (g'' \star g) \star g' \\ g'' \star e &= e \star g' \\ g'' &= g' \end{aligned}$$
for $g', g'' \in G$ two possibly different inverses of $g \in G$.

G is called an *abelian* group in case G also satisfies

4.
$$g \star h = h \star g$$
for all $g, h \in G$,

In many examples the operation $\star$ is called "multiplication" and is denoted by $\cdot$ (or simply juxtaposition), the identity is denoted by 1 ("one"), and the inverse of g by g^{-1}.

In cases where G is an abelian group, in many cases the operation $\star$ is denoted by $+$, the operation is called "addition", the identity is denoted 0 ("zero"), and the inverse of g is denoted by $-g$.

Definition 2. A *field* F is a non-empty set, together with two operations called *addition* and *multiplication*, denoted by $+$ and $\cdot$, respectively. They satisfy

1. F is an abelian group with respect to $+$ with identity element 0.
2. $F^* = F \setminus \{0\}$ is an abelian group with respect to $\cdot$ with identity element 1.
3. left and right distributive laws:

$$(x+y)z = xz + yz$$
$$x(y+z) = xy + xz$$

   for all $x, y, z \in F$.

Note in particular that $0 \neq 1$ in a field.

Remark 3. If this definition is altered by omitting commutativity for multiplication, one obtains the definition of a *skew field* or *division ring.* Many results of linear algebra still hold in this more general situation (e.g., solutions of systems of equations, matrices, row reduction, dimension of vector spaces) while others (e.g., eigenvalues, determinants) either no longer exist or take a substantially different form. We will not pursue this topic here.

Definition 4. An *associative ring* R is a non-empty set, together with two operations called *addition* and *multiplication*, denoted by $+$ and $\cdot$, respectively, which satisfy the following axioms:

1. R is an abelian group with respect to $+$ with identity element 0.
2. multiplication $\cdot$ is associative,
3. the left and right distributive laws hold.

Furthermore, we require that R has an *identity* element 1 which satisfies

$$1 \cdot x = x \cdot 1 = x$$

for all $x \in R$.

Note that it is no longer required that every non-zero element have a multiplicative inverse nor that multiplication be commutative. Thus $\mathbb{Z}$ (the integers), $F^{m\times m}$ (m by m matrices over a field F), and $F[x]$ (polynomials over a field F) are all associative rings.

It is easy to check that for any ring, the following hold:

1. $0\cdot r = r\cdot 0 = 0$ for all $r \in R$.
2. $(-1)\cdot r = r\cdot(-1) = -r$ for all $r \in R$.
3. $(-r)s = r(-s) = -(rs)$ for all $r, s \in R$.

E.g. for the first, compute $(0+0)\cdot r$ two different ways.

Definition 5. A ring R is *commutative*, if $xy = yx$ for all $x, y \in R$.

Definition 6. Let R be an associative ring (with identity). Let M be an additively written abelian group with identity element 0.

Then M is called a left R-*module*, if there is an operation

$$\begin{array}{rcl} \cdot : R\times M & \longrightarrow & M \\ (r,m) & \mapsto & r\cdot m \end{array}$$

for all $m \in M$ and for all $r \in R$ such that the following axioms hold:

1. $1\cdot m = m$
2. $(rs)\cdot m = r\cdot(s\cdot m)$
3. $r\cdot(m+n) = r\cdot m + r\cdot n$
4. $(r+s)\cdot m = r\cdot m + s\cdot m$

for all $m, n \in M$ and all $r, s \in R$.

One normally abbreviates $r\cdot m$ simply as rm.

One can define a right R-module in a similar manner by writing the element from the ring on the right. The concepts of left and right modules are different for non-commutative rings since condition 2. depends on the order of the operation in R.

Definition 7. Let F be a field and V be an abelian group written additively. V is a vector space over F simply means that V is an F-module.

Definition 8. Let R be a commutative ring. An R-module A which is also a ring such that the scalar multiplication and multiplication are compatible, that is, satisfy:

5. $r(ab) = (ra)b = a(rb)$ for all $r \in R$ and $a, b \in A$

is called an R-*algebra*.

Many of the R-algebras that we will consider are for the case where $R = F$ is a field. For example, $F[x]$ (polynomials), $F[[x]]$ (formal power series), and $F^{m \times m}$ for F a field are all F-algebras. The first two are commutative and for $m > 1$ the last one is not.

We have now given definitions of the main collections of objects that are studied in this course. The main content however is in the study of the functions which preserve the structures of these. We start with the first object defined.

Definition 9. Let G_1 and G_2 be groups. A function $f : G_1 \longrightarrow G_2$ is called a *group homomorphism* if $f(g \star h) = f(g) \star f(h)$ for all $g, h \in G_1$. Note that the first $\star$ denotes the operation in G_1 and the second $\star$ is that of G_2.

Note that it follows immediately that $f(e) = e$ where the first e is the identity of G_1 and the second the identity of G_2: Now

$$f(e) = f(e \star e) = f(e) \star f(e)$$

hence multiplying both sides by $f(e)^{-1}$ yields the result.

Definition 10. Let R_1 and R_2 be associative rings with identity. A *ring homomorphism* is a function $f : R_1 \longrightarrow R_2$ which satisfies

1. $f(r + s) = f(r) + f(s)$ for all $r, s \in R_1$.
2. $f(r \cdot s) = f(r) \cdot f(s)$ for all $r, s \in R_1$.
3. $f(1) = 1$.

A field homomorphism is just a special case of a ring homomorphism (a field is just a special type of ring).

Definition 11. Let M_1 and M_2 be modules over the same ring R (with 1). A function $f : M_1 \longrightarrow M_2$ is an R-*module homomorphism* if

1. $f(m + n) = f(m) + f(n)$ for all $m, n \in M_1$.
2. $f(r \cdot m) = r \cdot f(m)$ for all $r \in R$ and all $m \in M_1$.

Remark 12. If V_1 and V_2 are vector spaces over a field F, a linear transformation $T : V_1 \longrightarrow V_2$ is just an F-module homomorphism.

Definition 13. Let A_1 and A_2 be R-algebras over the commutative ring R (with 1). A function $f : A_1 \longrightarrow A_2$ is an R-*algebra homomorphism* if

1. f is an R-module homomorphism,
2. f is a ring homomorphism.

History of the Notes

The Notes for the course *Math 4330, Honors Linear Algebra* at Cornell University have been developed over the last ten years or so mainly by the following (in chronological order):

Gerhard O. Michler

R. Keith Dennis

Martin Kassabov

W. Frank Moore

Yuri Berest.

Harrison Tsai also contributed a number of interesting exercises that appear at the ends of several sections of the notes.

Most sections have been revised so many times the original author may no longer recognize it. The intent is to provide a modern treatement of linear algebra using consistent terminology and notation. Some sections are written simply to provide a central source of information such as those on "Useful Definitions", "Subobjects", and "Universal Mapping Properties" rather than as a chapter as one might find in a traditional textbook. Additionally there are sections whose intent is to provide proofs of some results which are not given in the lectures, but rather provide them as part of a more thorough development of a tangential topic (e.g., Zorn's Lemma to develop cardinal numbers and the existence of bases and dimension in the general case).

A large number of challenging exercises from many different sources have been included. Although most should be readily solvable by students who have mastered the material, a few even more challenging ones still remain.

Much still remains to be done. Corrections and suggestions for additional exercises, topics and supplements are always welcome.

Keith Dennis

e-mail address: **math4330@rkd.math.cornell.edu**

Fields

The notion of a field is central in linear algebra — one cannot talk about vector spaces without first specifying the field, that is, the collection of "numbers" that one is allowed to use. In some elementary textbooks it is assumed that all vector spaces are over the field of real numbers, however in this course we will consider vector spaces over arbitrary fields.

In general most of the results in linear algebra hold in the case of any field. One has to be aware that sometimes the cases of a finite field or a field of a positive characteristic need special attention.

Definition 1. A *field* is a set F together with two binary operations $+$ (addition) and $\cdot$ (multiplication), which satisfy the following axioms for all $a, b, c \in F$:

A1. Associativity of addition
$(a + b) + c = a + (b + c)$

A2. Commutativity of addition
$a + b = b + a$

A3. Existence of additive identity
There exists an element 0 such that $a + 0 = 0 + a = a$

A4. Existence of additive inverses
For any a there exists an element $-a$ such that $a + (-a) = (-a) + a = 0$
Notation: $b - a$ denotes $b + (-a)$

M1. Associativity of multiplication
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

M2. Commutativity of multiplication
$a \cdot b = b \cdot a$

M3. Existence of multiplicative identity
There exists an element $1 \in F$ such that $a \cdot 1 = 1 \cdot a = a$

M4. Existence existence of multiplicative inverses
For any $a \neq 0$ there exists an element a^{-1} such that $a \cdot (a^{-1}) = (a^{-1}) \cdot a = 1$

D. Distributive laws
$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and
$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

NT. Non-triviality
$1 \neq 0$

Remark 2. Another way to define a field is a set which is an abelian group with respect to addition and the set of all non-zero elements forms an abelian group with respect to multiplication; moreover the two operations are connected via the distributive laws.

The elements 0, 1, $-a$, a^{-1} mentioned above are in fact unique. See the handout "Some Useful Definitions" for a proof.

You may find different statements of the definition of field in other texts, but they are (almost) always equivalent to this one.

If the hypothesis M2 (commutativity of multiplication) is omitted, the resulting object is called a *division ring* or sometimes a *skew field*. See the exercises at the end for an example. It is actually possible to do a great deal of linear algebra with this more general assumption. We will not do so here however.

Example 3. 1. The sets $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers) and $\mathbb{C}$ (complex numbers) are fields with respect to the usual definitions of addition and multiplication.

2. Let i denote the complex number whose square is -1 and define

$$\mathbb{Q}[i] = \{\, a + bi \mid a, b \in \mathbb{Q} \,\} .$$

Clearly $\mathbb{Q}[i]$ is closed under addition and multiplication (check!) and since it is a subset of $\mathbb{C}$ containing both 0 and 1 it thus satisfies all of the axioms for a field except possibly the statement that every non-zero element has a multiplicative inverse which is in $\mathbb{Q}[i]$. We show now that it has that property as well. First note the usual computation with complex numbers:

$$(a + bi)(a - bi) = a^2 + b^2 \geq 0 ;$$

that is, the complex number times its complex conjugate is the sum of the squares of the the real and imaginary parts. Further, the square of a real number is always greater than or equal to 0 and hence the same is true of sum of the squares of two or more real numbers. We can now answer our question upon noting that $a + bi$ is 0 if and only if both a and b are 0. Thus if $a + bi$ is not zero, at least one of a or b is not 0 and so the sum of both squares $a^2 + b^2$ is strictly positive. Thus we now have a formula for the inverse of a non-zero element of $\mathbb{Q}[i]$:

$$\begin{aligned}(a + bi)^{-1} &= \frac{a - bi}{a^2 + b^2} \\ &= \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i ,\end{aligned}$$

which is in the correct form since each of $\frac{a}{a^2+b^2}$ and $\frac{-b}{a^2+b^2}$ is a rational number.

3. Let $\sqrt{3}$ denote the positive real number whose square is 3 and define

$$\mathbb{Q}[\sqrt{3}] = \left\{ a + b\sqrt{3} \;\middle|\; a, b \in \mathbb{Q} \right\} .$$

Clearly $\mathbb{Q}[\sqrt{3}]$ is closed under addition and multiplication (check!) and since it is a subset of $\mathbb{R}$ containing both 0 and 1 it thus satisfies all of the axioms for a field except possibly the statement that every non-zero element has a multiplicative inverse which is in $\mathbb{Q}[\sqrt{3}]$. We show now that it has that property as well. We make a computation analogous to the one in the previous example:

$$(a+b\sqrt{3})(a-b\sqrt{3}) = a^2 - b^2 3 \ .$$

However, this time it is a bit more difficult to understand when $a+b\sqrt{3}$ is non-zero since both terms are no longer positive. Note first that if $a^2-b^2 3=0$, then $a=0$ if and only if $b=0$. We wish to show that this is the only case in which $a+b\sqrt{3}$ is 0 when a and b are rational numbers. If $a^2-b^2 3=0$, then we have

$$\begin{aligned} a^2 &= 3b^2 \\ (\frac{a}{b})^2 &= 3 \ , \end{aligned}$$

that is, $\frac{a}{b}$ is a rational number whose square is 3. This is in fact not possible. We prove this by using the uniqueness of factorization of integers. Although this may be something you are already familiar with, we will prove it later in the course as such statements (about polynomials) will be relevant to the study of linear algebra. If $m \in \mathbb{Z}$ is a non-zero integer, this means that

$$m = \pm p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

where the p_i are distinct primes (a *prime* is an integer greater than 1 which can't be properly factored) and each n_i is a positive integer. Uniqueness means that there is only one such factorization for a given integer m (we ignore the order in which the p_i appear in the product). From this it follows that in the unique factorization of m^2, all primes appear with even exponents, that is, a prime appears in the factorization of m^2 if and only if it appears in the factorization of m. We state this as "if the prime p divides m^2, then p divides m". We can use this statement now to prove our previous assertion: $\sqrt{3}$ is not a rational number. For if it were we could write it as

$$\frac{m}{n} = \sqrt{3}$$

for some positive integers $m, n \in \mathbb{Z}$. Further, we may assume that the fraction is in lowest terms (that is, if a prime divides m it does not divide n and vice versa; m and n are said to be *relatively prime* in this case). We then have

$$m^2 = 3n^2$$

and since 3 divides m^2 it must divide m as noted above. So we can write $m = 3m'$ for some integer m'. Then we have

$$\begin{aligned} 9(m')^2 &= 3n^2 \\ 3(m')^2 &= n^2 \end{aligned}$$

and applying the same argument again: 3 divides n^2, so 3 also divides n. But this contradicts our assumption that m and n have no common factors. Thus we've shown that if $a + b\sqrt{3}$ is not 0, then $a^2 - 3b^2$ is not 0. We now have a formula for the inverse of a non-zero element of $\mathbb{Q}\sqrt{3}$:

$$\begin{aligned}(a + b\sqrt{3})^{-1} &= \frac{a - b\sqrt{3}}{a^2 - 3b^2} \\ &= \frac{a}{a^2 - 3b^2} + \frac{-b}{a^2 - 3b^2}\sqrt{3}\,,\end{aligned}$$

which is in $\mathbb{Q}[\sqrt{3}]$.

4. If p is a prime number, the collection of intgers modulo p is a field with p elements using the operations of addition and multiplication induced from the integers. This field is sometimes denoted by any of $\mathbb{Z}_p = \mathbb{F}_p = \mathrm{GF}(p)$.
   If you've not seen the integers modulo n before, they will appear shortly when we discuss equivalence relations.

5. We now give another example of a finite field. If there were a field with 4 elements, it would have to contain 0, 1 and two other elements. We call one of them α and further assume that the 0 and 1 behave as in the field with 2 elements, $\mathbb{F}_2$. In analogy with our earlier computations we write

$$\begin{aligned}\mathbb{F}_4 &= \mathbb{F}_2[\alpha] \\ &= \{\, a + b\alpha \mid a, b \in \mathbb{F}_2 \,\}\ .\end{aligned}$$

   As before it's clear that the sum of two elements in $\mathbb{F}_4$ will also be in $\mathbb{F}_4$. However, multiplying two elements of the given form using the distributive law will give an element of $\mathbb{F}_4$ only if α^2 is in $\mathbb{F}_4$. We now determine what might be possible. There are thus 4 possibilities:

$$\begin{aligned}\alpha^2 &= 0 \quad \textit{or} \\ \alpha^2 &= 1 \quad \textit{or} \\ \alpha^2 &= \alpha \quad \textit{or} \\ \alpha^2 &= 1 + \alpha\ .\end{aligned}$$

   Note that the first is not possible since α is different from 0 and $\mathbb{F}_4$ is to be a field. For the second we compute:

$$\begin{aligned}(\alpha + 1)^2 &= \alpha^2 + 2\alpha + 1 \\ &= \alpha^2 + 0 + 1 \\ &= 1 + 1 \\ &= 0\end{aligned}$$

   and thus $\alpha + 1 = 0$ or $\alpha = -1 = 1$ which is impossible since α is to be different from 0 and 1. Thus the only possibility is the last one, $\alpha^2 = 1 + \alpha$, or equivalently that α must be a root of the polynomial $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. One can now check directly that this definition will make the set $\mathbb{F}_4$ into a field. Later, we'll find ways to much more easily generalize this computation to construct many finite fields.

6. Notice that the set of all integers $\mathbb{Z}$ (with the usual operations) is **NOT** a field. Why?

Notation 4. Let F be a field. We can define a function $\phi : \mathbb{Z} \longrightarrow F$ as follows: for a positive number n we will denote the element $1 + 1 + \cdots + 1$ (the sum of n copies of the element 1) by $\phi(n)$. Similarly $\phi(-n)$ will denote the negative of the element $\phi(n)$. Often one abuses notation and denotes the element $\phi(n)$ simply with n, because they satisfy the "expected" properties (that is, ϕ is a ring homomorphism; see Exercise 4).

In the same way, for an element $x \in F$ and positive integer n, we can define x^n as the product of n copies of x. If the element x is not zero one can define x^{-n} as the inverse of x^n. Exercise 4 lists some properties of these "powers".

Definition 5. A function σ from a field F_1 to another field F_2 is called a *homomorphism* if it preserves the operations, i.e.

$$\begin{aligned} \sigma(a+b) &= \sigma(a) + \sigma(b) \\ \sigma(a \cdot b) &= \sigma(a) \cdot \sigma(b) \\ \sigma(1) &= 1\,. \end{aligned}$$

Here on the left $+$ and $\cdot$ denote the addition and multiplication in the field F_1 and on the right the corresponding operations in field F_2.

If the two fields F_1 and F_2 are the same and σ is a bijection, then σ is called an *automorphism*.

Remark 6. Any function between fields which preserves addition and multiplication automatically sends 0 to 0. In fact, unless the function sends everything to 0 it must also send 1 to 1. Verify this statement.

Definition 7. A subset K of a field F is called a *subfield*, if it is a field with respect to the inherited operations. The field F is also called an *extension* field of K.

Remark 8. This definition is equivalent to the statement that K contains the elements 0 and 1 and is closed under addition, multiplication, and taking negatives and inverses. Verify.

It can be shown that for any subset S of F there exists a minimal (with respect to inclusion) subfield K of F which contains S (see Exercise 7). One very important case is when the set S is empty, i.e., every field F contains a unique minimal subfield. This subfield is called the *prime* subfield. There are only a few possible isomorphism types of prime subfields (see Exercise 8).

Definition 9. For a field F (or more generally for any ring containing 1) we say that F has *characteristic* n if n is the smallest positive integer so that $1 + 1 + \cdots + 1 = 0$ (n copies of 1). If no such n exists, F is said to have *characteristic* 0. We denote this by either $\operatorname{char} F = n$ or $\operatorname{char} F = 0$.

Remark 10. In general any positive integer is possible for the characteristic of a ring (give examples). If the ring has no zero-divisors, i.e., non-zero elements a, b with $ab = 0$, then one can easily show that the characteristic must be either 0 or a prime number.

For example $\mathbb{F}_p$ for a prime p has characteristic p and $\mathbb{Q}$ has characteristic 0.

Exercise 8 shows that every prime subfield is one of the examples just given.

Definition 11. Let F be a field of positive characteristic p. The function $\sigma : F \longrightarrow F$ defined by $\sigma(x) = x^p$ is called the *Frobenius* homomorphism. [Verify that this function is indeed a homomorphism.]

Definition 12. A field is called **perfect** if it has characteristic 0 or the Frobenius homomorphism is an automorphism, i.e., it is surjective. Why is it always injective?.

Exercises

Fields 1. Construct a field F with 9 elements (give its addition and multiplication table). [Hint: Try $\mathbb{F}_9 = \mathbb{F}_3[\beta]$ where $\ldots$].

Fields 2. Does there exist a field with 6 elements? If so, give its addition and multiplication table. If not, give a proof.

Fields 3. Verify that addition and multiplication are well defined operations in $\mathbb{F}_p$. Also verify that they satisfy all the axioms.

Fields 4. a. Verify that addition and multiplication in any field F and in the integers are compatible, i.e., consider the function $\phi : \mathbb{Z} \longrightarrow F$, which sends n to n

$$\phi(n) + \phi(m) = \phi(n + m) \qquad \phi(n) \cdot \phi(m) = \phi(nm),$$

which is the same as saying that the function $\phi : \mathbb{Z} \longrightarrow F$ is a ring homomorphism (we have not defined rings and ring homomorphism yet).

b. Verify that if $x \neq 0$, then

$$x^n \cdot x^m = x^{n+m} \qquad (x^n)^m = x^{nm} \qquad (x^n)^{-1} = x^{-n},$$

which is the same as saying that the function $\psi : \mathbb{Z} \longrightarrow F^*$, which sends n to x^n is a group homomorphism. Here F^* denotes the multiplicative group of the field F, i.e., the set of all non-zero elements with respect to multiplication.

Fields 5. Let $\sigma : F_1 \longrightarrow F_2$ be a function from one field to another which preserves addition, multiplication, and is non-trivial (that is, there exists an element $a \in F_1$ with $\sigma(a) \neq 0$), then σ is a homomorphism.

Fields 6. Show that any homomorphism between two fields is one-to-one, i.e., $\sigma(a) = \sigma(b)$ implies $a = b$.

Fields 7. Let F be a field and S be a subset of F. Show that there is a unique minimal subfield of F which contains all elements from S. All elements in this subfield can be obtained from the elements in S together with 1 using finitely many operations (addition, subtraction, multiplication and inversion).

Fields 8. a. Show that the prime subfield of F consists of all elements which can be written as $a \cdot b^{-1}$ where a and $b \neq 0$ are multiples of 1, i.e., elements like $\phi(n)$ for some integer n.

b. Show that any prime subfield is isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$.

Fields 9. An equivalent way to define characteristic of a field is as follows: Let F be a field. Consider the function $\phi : \mathbb{Z} \longrightarrow F$, which sends n to $1 + 1 + \cdots + 1$ (n times). If this function is injective, then we say that $\operatorname{char} F = 0$. Otherwise $\operatorname{char} F$ is the smallest positive integer which is sent to 0 by the function ϕ. Using this definition show that $\operatorname{char} F$ is a prime number.

Fields 10. Let $\sigma : F_1 \longrightarrow F_2$ be a homomorphism where F_1 and F_2 are fields. Show σ induces an isomorphism between their prime subfields, and, in particular, the characteristics of F_1 and F_2 are the same.

Fields 11. Show that the Frobenius map σ defined in Definition 11 is indeed a homomorphism.

Fields 12. Show that any finite field is perfect.

Fields 13. Let $\mathbb{Q}[\sqrt{2}]$ denote the set of all elements in $\mathbb{C}$ which can be written as $a + b\sqrt{2}$, where a and b are rational numbers.

a. Show that $\mathbb{Q}[\sqrt{2}]$ is the smallest subfield of $\mathbb{C}$ which contains $\sqrt{2}$. Further, show that it is strictly larger than $\mathbb{Q}$.

b. Describe all automorphisms of $\mathbb{Q}[\sqrt{2}]$.

c. One can replace $\sqrt{2}$ with $\sqrt{d}$ where d is any rational number. If d is not a perfect square, the answer to part a) is the same. However if d is a perfect square the answer is different. Why?

Fields 14. Let $p > 1$ be a prime number. Show that

$$\mathbb{Q}(\sqrt{p}) = \{\, a + b\sqrt{p} \mid a, b \in \mathbb{Q} \,\}$$

is a subfield of the field $\mathbb{R}$ of real numbers which contains $\mathbb{Q}$ properly. What is $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{p})$ for any odd prime p?

Fields 15. a. Let $\mathbb{Q}[\sqrt[3]{2}]$ denote the minimal subfield of $\mathbb{C}$ which contains $\sqrt[3]{2}$ (the positive real number whose cube is equal to 2). Give an explicit description of this field (as a set) and show directly that it is a field.

b. Let $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ denote the minimal subfield of $\mathbb{C}$ which contains $\sqrt{2}$ and $\sqrt{3}$. Give an explicit description of this field (as a set) and show directly that it is a field. Further, prove that it is strictly larger than both $\sqrt{2}$ and $\sqrt{3}$.

c. Find all automorphisms of $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Fields 16. In this exercise you may use standard results about real and complex numbers (as well as what you've learned in class).

a. Let $\mathbb{Q}[\sqrt[3]{3}]$ denote the minimal subfield of $\mathbb{C}$ which contains $\sqrt[3]{3}$ (the positive real number whose cube is equal to 3). Give an explicit description of this field (as a set) and show directly that it is a field.

b. Let $\mathbb{Q}[\sqrt{3}, \sqrt{5}]$ denote the minimal subfield of $\mathbb{C}$ which contains $\sqrt{3}$ and $\sqrt{5}$. Give an explicit description of this field (as a set) and show directly that it is a field.

c. Find all automorphisms of $F = \mathbb{Q}[\sqrt{3}, \sqrt{5}]$. [Hint: If α is an automorphism of F what can you say about the value of $\alpha(\sqrt{3})$?]

Fields 17. a. Show that any automorphism of $\mathbb{Q}$ is trivial.

b. Show that any automorphism of $\mathbb{R}$ is trivial.

Warning: A similar statement in the case of $\mathbb{C}$ is **FALSE**. In fact the field of complex numbers has uncountably many automorphisms - for example complex conjugation is one automorphism of $\mathbb{C}$.

Fields 18. Show that there exist fields with 9 and 25 elements (give the addition and multiplication tables). Can you show that any two fields with 9 elements are isomorphic?
Hint: Use an element which behaves like $\sqrt{2}$.

Fields 19. Show that $1 + \sqrt{2} + \sqrt{3} + \sqrt{6} \in \mathbb{R}$ has a multiplicative inverse of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ where $a, b, c, d \in \mathbb{Q}$. (**Note:** In fact,

$$\left\{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \;\middle|\; a, b, c, d \in \mathbb{Q} \right\}$$

is actually a field. We will be able to show this after studying (perhaps surprisingly) polynomials.)

Fields 20. Let F be a field. Let $F(t)$ denote the set of all rational functions with coefficients in F, i.e., the set of all formal fractions

$$\frac{a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0}{b_m t^m + b_{m-1} t^{m-1} + \cdots + b_1 t + b_0}$$

where a_i and b_j are elements in F and $b_m \neq 0$. Two fractions $f(t)/g(t)$ and $p(t)/q(t)$ are equal if $f(t)q(t) = g(t)p(t)$ as polynomials in t. Show that $F(t)$ is a field with respect to the natural addition and multiplication. This field is called the **field of rational functions** in one variable over F. Notice that F can be viewed as a proper subfield of $F(t)$.

Remark: This example will be given a precise description when we study equivalence relations.

Fields 21. Give an example of a non-surjective homomorphism from $F(t)$ to $F(t)$, which preserves the subfield F.

Fields 22. Let F be a field. Let $F((t))$ be the set of all formal power series with finitely many negative terms, i.e.,

$$a_{-n}t^{-n} + a_{-n+1}t^{-n+1} + c\cdots + a_0t^0 + a_1t^1 + a_2t^3 + \cdots + a_kt^k + \cdots,$$

where a_i are elements in F. Show that $F((t))$ is a field with respect to the natural addition and multiplication. This field is called the **field of Laurent series** over F. Notice that F can be viewed as a proper subfield of $F((t))$.

There is a homomorphism θ from the field of rational functions $F(t)$ to the field of Laurent series. The homomorphism θ sends the elements in $F \subseteq F(t)$ to the corresponding ones in $F \subseteq F((t))$ and sends t to t. The properties of θ uniquely determine the values of θ on other elements in $F(t)$ (verify). For example, show that

$$\theta\left(\frac{1}{1-t}\right) = 1 + t + t^2 + t^3 + \cdots + t^n + \cdots$$

Show that this homomorphism is **NEVER** surjective. It allows one to consider $F(t)$ as a proper subfield of $F((t))$.

Fields 23. Give an example of a field which is not perfect.

Fields 24. Give examples of fields F such that:

1. F is isomorphic to $F(t)$;
2. F is isomorphic to $F((t))$;
3. $F(t)$ is isomorphic to $F((t))$.

Fields 25. a. Let R be a commutative ring containing with no non-zero elements a, b satisfying $ab = 0$. In this case we say that R has no *zero-divisors.* If R is finite, contains 1 and $0 \neq 1$, prove that R is a field.

b. In the previous part, do not assume that 1 is in R, but only that R has at least 2 elements. Show that R must be a field.

c. Let F be a field and assume $F \subseteq R$ with R a commutative ring having no zero-divisors. Assume that the addition and multiplication of elements of F is the same when the elements are considered as being in F or in R. (R is an F-algebra.)
Show that if R considered as a vector space over F has finite dimension, then R must be a field.

d. In the previous part do not assume that R is commutative, but only that the dimension is finite. Show that every non-zero element of R must have a multiplicative inverse.

Fields 26. Let F be a field with $\mathbb{Q} \subseteq F$. If F considered as a vector space over $\mathbb{Q}$ has dimension 2, show that there exists an element $a \in F$ which is not in $\mathbb{Q}$ which satisfies an equation of the form $a^2 - n = 0$ for some non-zero integer n. Conclude that F is isomorphic to $\mathbb{Q}[\sqrt{n}]$. Show further that we may assume n is *square-free*: if p is a prime that divides n, then p^2 does not divide n.

Fields 27. Let F be a field. Let R be the set of 2×2 matrices of the form

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

for a, b in F with the usual matrix operations.

a. Show that R is a commutative ring with 1 and the set of diagonal matrices are naturally isomorphic to F.

b. For which of the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_5$, $\mathbb{F}_7$ is R a field?

c. Characterize which elements of R have a multiplicative inverse.

d. Characterize the fields F for which R will be a field.

e. For which $\mathbb{F}_p$ (p prime) is R a field?

Fields 28. Let F be a field. Let $R = \mathbb{H}(F)$ be the vector space of dimension 4 over F with basis $\{1, i, j, k\}$, so a typical element will look like $z = a\cdot 1 + b\cdot i + c\cdot j + d\cdot k$. Define multiplication on this vector space by the rules

1. $i^2 = j^2 = k^2 = -1$,
2. $ij = k = -ji$,
3. $jk = i = -kj$,
4. $ki = j = -ik$,
5. $ai = ia$, $aj = ja$, $ak = ka$ for all $a \in F$
6. $1z = z1 = z$ for all $z \in R$,

and extend to all of R by the distributive laws. Then $\mathbb{H}(F)$ is a non-commutative ring for any field F. It is called the ring of *quaternions* over F. Define the function

$$\bar{\ }: R \longrightarrow R$$

by $\overline{z} = a \cdot 1 - b \cdot i - c \cdot j - d \cdot k$. The element $\overline{z}$ is called the *quaternion conjugate* of z.

1. Verify the formula
$$z \cdot \overline{z} = \overline{z} \cdot z = a^2 + b^2 + c^2 + d^2 .$$
2. Show that if $F = \mathbb{R}$ or $\mathbb{Q}$, then $\mathbb{H}(F)$ is a division ring.
3. For which of the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_5$, $\mathbb{F}_7$ is R a division ring?
4. Characterize which elements of R have a multiplicative inverse.
5. Characterize the fields F for which R will be a division ring.
6. For which $\mathbb{F}_p$ (p prime) is R a division ring?

Fields 29. Let F be a field and let $H(F)$ denote the set of all 4×4 matrices of the form

$$f(z) = \begin{bmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{bmatrix}$$

for $a, b, c, d \in F$. Define

$$f : \mathbb{H}(F) \longrightarrow H(F)$$

via the above matrix for $z = a \cdot 1 + b \cdot i + c \cdot j + d \cdot k$. Verify that f is a one-to-one, onto function which satisfies

$$f(z + w) = f(z) + f(w)$$

and

$$f(zw) = f(z)f(w)$$

for all $z, w \in \mathbb{H}(F)$ and $f(1)$ is the identity matrix. That is, f is an isomorphism of rings. Read the section "The Matrix of a Linear Transformation" and explain explicitly what gives the isomorphism f.

Fields 30. Let $\mathbb{H} = \mathbb{H}(\mathbb{R})$. $\mathbb{H}$ is called the division ring of real quaternions. Decompose $\mathbb{H}$ as the direct sum of a 1-dimensional and 3 dimensional vector space over $\mathbb{R}$:

$$\mathbb{H} = \mathbb{R} \oplus V$$

where V is the span of $\{i, j, k\}$ over $\mathbb{R}$. We may thus think of elements of $\mathbb{H}$ as pairs (a, v) where $a \in \mathbb{R}$ and $v \in \mathbb{R}^3$. Explicitly describe the multiplication

$$(a, u) \cdot (b, v)$$

in $\mathbb{H}$ and interpret it in terms of the usual definitions of

1. multiplication in $\mathbb{R}$,
2. scalar product (from left)
$$\mathbb{R} \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3 \ ,$$
3. scalar product (from right)
$$\mathbb{R}^3 \times \mathbb{R} \longrightarrow \mathbb{R}^3 \ ,$$
4. dot product
$$\cdot : \ \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R} \ ,$$
5. cross product
$$\times : \ \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3 \ .$$

Look up the history of the quaternions, find out what they have to do with rotations in $\mathbb{R}^3$, and why one of their first applications was in physics. The latter application is now usually replaced by the standard vector space operations just listed above.

History of the Notes

The Notes for the course *Math 4330, Honors Linear Algebra* at Cornell University have been developed over the last ten years or so mainly by the following (in chronological order):

Gerhard O. Michler

R. Keith Dennis

Martin Kassabov

W. Frank Moore

Yuri Berest.

Harrison Tsai also contributed a number of interesting exercises that appear at the ends of several sections of the notes.

Most sections have been revised so many times the original author may no longer recognize it. The intent is to provide a modern treatement of linear algebra using consistent terminology and notation. Some sections are written simply to provide a central source of information such as those on "Useful Definitions", "Subobjects", and "Universal Mapping Properties" rather than as a chapter as one might find in a traditional textbook. Additionally there are sections whose intent is to provide proofs of some results which are not given in the lectures, but rather provide them as part of a more thorough development of a tangential topic (e.g., Zorn's Lemma to develop cardinal numbers and the existence of bases and dimension in the general case).

A large number of challenging exercises from many different sources have been included. Although most should be readily solvable by students who have mastered the material, a few even more challenging ones still remain.

Much still remains to be done. Corrections and suggestions for additional exercises, topics and supplements are always welcome.

Keith Dennis

e-mail address: **math4330@rkd.math.cornell.edu**