Math 541

Crude Summary of Lectures

September 6, 2000

1 Fields

§1 Note the analogy between the laws of addition and the laws of multiplication.

$a+b=b+a$	$ab=ba$
$(a+b)+c=a+(b+c)$	$(ab)c=a(bc)$
$a+0=a$	$a\cdot 1=a$
$a+(-a)=0$	$a\cdot a^{-1}=1$
$a-b=a+(-b)$	$a/b=a\cdot b^{-1}$
$a-b=(a+c)-(b+c)$	$a/b=(ac)/(bc)$
$(a-b)+(c-d)=(a+c)-(b+d)$	$(a/b)\cdot(c/d)=(ac)/(bd)$
$(a-b)-(c-d)=(a+d)-(b+c)$	$(a/b)/(c/d)=(ad)/(bc)$

The last line explains why *we invert and multiply to divide fractions.*

§2 Definition. A **field** is a set F equipped with two binary operations

$$F\times F\to F:(a,b)\mapsto a+b \qquad \textbf{(addition)}$$
$$F\times F\to F:(a,b)\mapsto a\cdot b \qquad \textbf{(multiplication)}$$

and two distinguished elements 0 (**zero**) and 1 (**one**) which satisfies the following laws:

Addition is associative:

$$\forall a\forall b\forall c \quad (a+b)+c=a+(b+c)$$

Addition is commutative:

$$\forall a \forall b \quad a + b = b + a$$

0 is an additive identity:

$$\forall a \quad a + 0 = a$$

Every number has an additive inverse:

$$\forall a \exists b \quad a + b = 0.$$

Multiplication is associative:

$$\forall a \forall b \forall c \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Multiplication is commutative:

$$\forall a \forall b \quad a \cdot b = b \cdot a$$

1 is an multiplicative identity:

$$\forall a \quad a \cdot 1 = 1 \cdot a = a$$

Every nonzero number has an multiplicative inverse:

$$\forall a \neq 0 \exists b \quad a \cdot b = b \cdot a = 1.$$

Multiplication is distributive over addition:

$$\forall a \forall b \forall c \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$

$$\forall a \forall b \forall c \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

(This is the first law which involves both operations.)

§3 Lemma. $a + b_1 = 0$ and $a + b_2 = 0 \implies b_1 = b_2$

Proof: Assume $a + b_1 = 0$ and $a + b_2 = 0$. Then

$$\begin{aligned} b_1 &= b_1 + 0 && \text{(ident.)} \\ &= b_1 + (a + b_2) && \text{(hyp.)} \\ &= (b_1 + a) + b_2 && \text{(ass.)} \\ &= (a + b_1) + b_2 && \text{(comm.)} \\ &= 0 + b_2 && \text{(hyp.)} \\ &= b_2 + 0 && \text{(comm.)} \\ &= b_2 && \text{(ident.)} \end{aligned}$$

§4 Definition. Since a number a has exactly one additive inverse we can denote it by $-a$. Thus

$$b = -a \iff a + b = 0.$$

The operation of **subtraction** is defined by

$$a - b = a + (-b).$$

§5 Theorem. $-(-a) = a$ for all $a \in F$.
Proof: $(-a)+a = a+(-a) = 0$ and $(-a)+(-(-a)) = 0$. Now use lemma 3.
□

§6 Exercise. Prove the following for all $a, b, c, d \in F$:

1. $-(a + b) = (-a) + (-b)$
2. $(a - b) + (c - d) = (a + c) - (b + d)$
3. $a - b = (a + c) - (b + c)$
4. $(a - b) - (c - d) = (a - b) + (d - c)$

§7 Lemma. The multiplicative inverse is unique:

$$a \cdot b_1 = 1 \text{ and } a \cdot b_2 = 1 \implies b_1 = b_2$$

Proof: Like Lemma 3.

§8 Definition. We denote the multiplicative inverse by a^{-1}. Hence for $a, b \in F$

$$b = a^{-1} \iff a \cdot b = 1.$$

The operation of **division** is defined (for $a \in F$, $b \in F \setminus \{0\}$) by

$$a/b = a \cdot b^{-1}.$$

§9 Theorem. $(a^{-1})^{-1} = a$ for $a \in F \setminus \{0\}$.
Proof: Like theorem 5.

§10 Exercise. Prove the following for all $a, b, c, d \in F \setminus \{0\}$:

1. $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$

2. $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$

3. $\frac{a}{b} = \frac{a \cdot c}{b \cdot c}$

4. $\frac{a}{b} \Big/ \frac{c}{d} = \frac{a}{b} \cdot \frac{d}{c}$

(Hint: compare with exercise 6.

§11 Theorem. $a \cdot 0 = 0$ for $a \in F$.

Proof: Choose $a \in F$. Then

$$
\begin{aligned}
0 &= a - a && \text{(def, inv.)} \\
&= a \cdot 1 - a && \text{(ident.)} \\
&= a \cdot (0 + 1) - a && \text{(ident, comm.)} \\
&= (a \cdot 0) + (a \cdot 1)) - a && \text{(dist.)} \\
&= ((a \cdot 0) + a) - a && \text{(ident.)} \\
&= (a \cdot 0) + (a - a) && \text{(ass.)} \\
&= (a \cdot 0) + 0 && \text{(def, inv.)} \\
&= a \cdot 0 && \text{(ident.)}\Box
\end{aligned}
$$

§12 Exercise. Prove the following

1. $\frac{a}{b} + \frac{c}{d} = \frac{(a \cdot d) + (c \cdot b)}{b \cdot d}$

2. $-a = (-1) \cdot a$

3. $(-a) \cdot (-b) = a \cdot b$

§13 Exercise. Each of the following sets F has operations of addition and multiplication (and a zero and one) which you have studied in grade school or high school. For each specify which of the field laws hold.

(i) The set $\mathbb{N}$ of nonnegative integers.

(ii) The set $\mathbb{Z}$ of integers.

(iii) The set $\mathbb{Q}$ of rational numbers.

(iv) The set $\mathbb{R}$ of real numbers.

(v) The set $\mathbb{C}$ of complex numbers.

(vi) The set $\mathbb{R}[x]$ of polynomials with real coefficients. A typical element of $\mathbb{R}[x]$ is a function f of form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where the coefficients $a_0, a_1, a_2 \ldots, a_n \in \mathbb{R}$.

(vii) The set $\mathbb{R}(x)$ of rational functions with real coefficients. A typical element of $\mathbb{R}(x)$ is a function f of form

$$f(x) = \frac{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n}{b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m}$$

where the coefficients $a_0 \ldots, b_m \in \mathbb{R}$ and at least one of the coefficients $b_0, b_1, b_2 \ldots, b_m$ is not zero.

(viii) The set $\mathbb{R}^{2\times 2}$ of 2×2 matrices. A typical element A of $\mathbb{R}^{2\times 2}$ has form

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$.

§14 First Homework. The above exercises and Herstein: 1.1.2, 1.2.9, 1.2.13, 1.3.5, 1.3.7, 1.3.8, 1.3.10, 1.3.12. 1.3.19, 1.4.1, 1.4.7, 1.4.9, 1.4.10, 1.4.11.