FOREWORD

The completion of this course will provide the conscientious student with a knowledge of the important properties of fields and of ordered fields, and of the techniques for handling the three most important examples: the rational numbers, the real numbers, and the complex numbers. The course will thus serve as the foundation for a later course in applied algebra, which covers such topics as theory of equations and matrix algebra, or for a later course in pure algebra, which covers such topics as groups, rings, and vector spaces. When followed by companion courses in trigonometry and analytical geometry, this course will also serve as a foundation for the study of calculus.

In principle, this course presupposes nothing from the student's previous training except the ability to read and to compute sums and products of positive integers. In practice, some previous exposure to fractions, to negative integers, and to the general notion of using letters to represent numbers would be helpful, but not at all necessary.

A great deal of attention has been devoted in this course to the elementary notions of logic. Such attention at this stage in the student's development will be amply justified by his confidence in later encounters with mathematics; for the logical structure of the subject, once grasped, will facilitate his reconstruction of individual facts and formulas. The "programmed" presentation enables the student to participate personally in the deduction from axioms of all the necessary theorems of the "language of elementary algebra" (the mathematician will recognize the semi-formal system to which we have given that name to be the theory of fields of characteristic 0.)

Most of the figures in the supplementary book are designed to serve as concise summaries of material which is explained in greater detail in the program itself. The student is referred to these figures at appropriate points throughout the program, and he is encouraged to use them for review and reference thereafter whenever necessary.

F. William Lawvere

TABLE OF CONTENTS

Figure 1

EXPRESSIONS

1. Basic expressions:

   a. 0 is an expression.

   b. Each positive integer 1, 2, 3, 4, ... is an expression.

   c. Each variable a, b, x, y, ... is an expression.

2. Algebraic operations:

   *a. If α represents any expression and if β represents any expression, then

   $$(\alpha)+(\beta)$$

   is an expression called the sum of the expressions α, β.

   **b. If α represents any expression and if β represents any expression, then

   $$(\alpha)(\beta)$$

   is an expression called the product of the expressions α, β.

   c. If α represents any expression, then

   $$-(\alpha)$$

   is an expression called the negative of the expression α.

   d. If α represents any expression, then

   $$\frac{1}{(\alpha)}$$

   is an expression called the reciprocal of the expression α.

3. All expressions are constructed from the basic expressions by repeated use of the algebraic operations mentioned in 2.

Notes: *We call the expressions α, β the terms of the sum $(\alpha)+(\beta)$.

**We call the expressions α, β the factors of the product $(\alpha)(\beta)$.

Greek letters such as α, β, γ, δ, ϵ (alpha, beta, gamma, delta, epsilon) are used throughout the course to represent expressions.

Square brackets are sometimes substituted for parentheses to achieve greater clarity, e.g.

$[(a+b)+c]+(x+y)$ means the same as $((a+b)+c)+(x+y)$, $(a+b)[(x+y)(u+(-v))]$ means the same as $(a+b)((x+y)(u+(-v)))$.

Pairs of parentheses ( ) and square brackets [ ] are treated exactly alike. The only purpose in using both is to avoid confusion in identifying pairs of them.

Figure 2

ABBREVIATION OF EXPRESSIONS

1. Omission of Parentheses:

   a. If one of the terms of a sum happens to consist only of a basic expression, then we neglect to enclose it in parentheses, e.g.

$$x+(\beta) \text{ instead of } (x)+(\beta)$$
$$(\alpha)+3 \text{ instead of } (\alpha)+(3)$$
$$x+y \text{ instead of } (x)+(y)$$

   b. If one of the factors of a product happens to consist only of a variable, then we neglect to enclose it in parentheses, e.g.

$$a(\beta) \text{ instead of } (a)(\beta)$$
$$(\alpha)x \text{ instead of } (\alpha)(x)$$
$$xy \text{ instead of } (x)(y)$$

   If only one of the factors is a positive integer, the same convention applies, e.g.

$$3(\beta) \text{ instead of } (3)(\beta)$$
$$5x \text{ instead of } (5)(x)$$

   But if both factors are positive integers, we must either retain the parentheses or use a dot in order to avoid confusion, e.g.

$$2\cdot 3 \text{ or } (2)(3) \text{ but not } 23$$
$$6\cdot 8 \text{ or } (6)(8) \text{ but not } 68$$

   c. Parentheses are omitted in forming the negative of a basic expression, e.g.

$$-4 \text{ instead of } -(4)$$
$$-x \text{ instead of } -(x)$$

   d. In forming the reciprocal of any expression which is not itself a reciprocal, we neglect to enclose that expression in parentheses, e.g.

$$\frac{1}{(\alpha)+(\beta)} \text{ instead of } \frac{1}{((\alpha)+(\beta))}$$
$$\frac{1}{x} \text{ instead of } \frac{1}{(x)}$$
$$\frac{1}{(\alpha)(\beta)} \text{ instead of } \frac{1}{((\alpha)(\beta))}$$
$$\frac{1}{-(\alpha)} \text{ instead of } \frac{1}{(-(\alpha))}$$

   However $\dfrac{1}{\left(\dfrac{1}{(\alpha)+(\beta)}\right)}$, $\dfrac{1}{\left(\dfrac{1}{(\alpha)(\beta)}\right)}$, etc. retain the parentheses.

(cont'd on page 3)

Figure 2 (cont'd)

ABBREVIATION OF EXPRESSIONS

1. Omission of Parentheses: (Continued)

   e. If a term of a sum is itself a product, we neglect to enclose that term in parentheses, e.g.
   $$(\alpha)(\beta)+(\gamma) \text{ instead of } ((\alpha)(\beta))+(\gamma)$$

   f. If a term of a sum is itself a reciprocal or a fraction (see 3b below), we neglect to enclose that term in parentheses, e.g.
   $$\frac{1}{3}+(\alpha) \text{ instead of } \left(\frac{1}{3}\right)+(\alpha)$$
   $$\frac{a}{b}+\frac{c}{d} \text{ instead of } \left(\frac{a}{b}\right)+\left(\frac{c}{d}\right)$$

*2. Omission of parentheses permitted by associative axioms:

   a. $(\alpha)+(\beta)+(\gamma)$ instead of $((\alpha)+(\beta))+(\gamma)$ or $(\alpha)+((\beta)+(\gamma))$

   b. $(\alpha)(\beta)(\gamma)$ instead of $((\alpha)(\beta))(\gamma)$ or $(\alpha)((\beta)(\gamma))$

3. Abbreviations which define new operations:

   a. $(\alpha)-(\beta)$ instead of $(\alpha)+[-(\beta)]$

   b. $\dfrac{(\alpha)}{(\beta)}$ instead of $(\alpha)\left(\dfrac{1}{(\beta)}\right)$

   **c. $(\alpha)^1$ instead of α
   $(\alpha)^{n+1}$ instead of $(\alpha)[(\alpha)^n]$ where n is any positive integer

   ***d. $(\alpha)^0$ instead of 1
   $(\alpha)^{-1}$ instead of $\dfrac{1}{(\alpha)}$
   $(\alpha)^{-n}$ instead of $[(\alpha)^{-1}]^n$, i.e. instead of $\left(\dfrac{1}{(\alpha)}\right)^n$
   where n is any positive integer

4. An abbreviation of an expression is also referred to as an expression.

Notes: *Each of α, β, γ, δ is said to be a term of the expression $(\alpha)+(\beta)+(\gamma)+(\delta)$.
Similarly, each of α, β, γ, δ is said to be a factor of the expression $(\alpha)(\beta)(\gamma)(\delta)$.

**3c is an "inductive definition." For any fixed positive integer m and expression α, the meaning of $(\alpha)^m$ can be discovered by an m-step process in which the first step is the first line of 3c, and in which the remaining steps have the form of the second line of 3c, where successively $n=1, n=2, \ldots, n=m-1$. Many of the parentheses in the result can be dropped by 2b. For example, $(\alpha)^5=(\alpha)(\alpha)(\alpha)(\alpha)(\alpha)$.

***The abbreviated expressions defined in 3d do not represent numbers if the expression α represents the number 0.

Figure 3

STATEMENTS

1. Basic Statements:

   If α represents any expression and if β represents any expression, then
$$\alpha = \beta$$
   is a statement called an equation.

2. Logical Operations:

   a) If P represents any statement and if Q represents any statement, then the following is also a statement:
$$(P) \textit{ and } (Q)$$

   b) If P represents any statement and if Q represents any statement, then the following is also a statement:
$$(P) \textit{ or } (Q)$$

   *c) If P represents any statement, then
$$\textit{not } (P)$$
   is also a statement.

   **d) If P represents any statement and if Q represents any statement, then
$$(P) \Rightarrow (Q)$$
   is a statement called a conditional statement.

   ***e) If x is any variable and if $P(x)$ represents any statement containing one or more occurrences of the variable x, then
$$\forall x,\ P(x)$$
   is a statement called a general statement.

3. All statements in the language of elementary algebra are constructed from equations by repeated use of the logical operations mentioned in 2.

Notes: *If P represents the equation $\alpha = \beta$, then "*not P*" is denoted by $\alpha \neq \beta$.

**A conditional statement $P \Rightarrow Q$ is read either "*if P, then Q*" or "*P implies Q*." P is called the hypothesis and Q is called the conclusion of $P \Rightarrow Q$.

***A general statement $\forall x$, $P(x)$ is read "*for every number x*, $P(x)$."

"$P \Leftrightarrow Q$" is used as an abbreviation for the statement "$(P \Rightarrow Q)$ *and* $(Q \Rightarrow P)$." If $P \Leftrightarrow Q$ is true, then P, Q are said to be logically equivalent.

We do not state explicitly the conventions for abbreviating statements by omitting parentheses; these conventions are analogous to those for expressions. Although we use such abbreviations, the logical structure which we intend should always be clear.

Figure 4

RULES OF INFERENCE

1. Rule of Inference for Conditional Statements:
   Let P represent any statement and let Q represent any statement. *Then we may infer the statement Q from the pair of statements*

$$P \Rightarrow Q,\ P.$$

*2. Rule of Inference for General Statements:
   Consider the general statement $\forall x\ \forall y \cdots \forall z,\ P(x, y, \cdots, z)$ in which $P(x, y, \cdots, z)$ represents any statement which does not contain the smybol $\forall$ and which does contain one or more occurrences of each of the variables $x, y, \cdots, z$. Let $\alpha, \beta, \cdots, \gamma$ represent any expressions. Let $P(\alpha, \beta, \cdots, \gamma)$ denote the statement obtained by substituting the expressions

$$\begin{array}{l} \alpha \text{ for each occurrence of the variable } x \text{ in } P(x, y, \cdots, z), \\ \beta \text{ for each occurrence of the variable } y \text{ in } P(x, y, \cdots, z), \\ \vdots \\ \gamma \text{ for each occurrence of the variable } z \text{ in } P(x, y, \cdots, z). \end{array}$$

   Then we may infer the statement $P(\alpha, \beta, \cdots, \gamma)$ from the general statement

$$\forall x\ \forall y \cdots \forall z,\ P(x, y, \cdots, z).$$

**3. Rule of Inference for Deductions:
   A list $Q_1, Q_2, Q_3, \cdots, Q$ of statements is said to be a deduction (of its last statement Q) from a certain collection of assumption-statements provided that each of the statements $Q_1, Q_2, Q_3, \cdots, Q$ in the list is either one of the assumptions, a true statement, or is inferred from previous statements in the list by means of one of the four rules of inference. *We may infer the conditional statement $P \Rightarrow Q$ from any deduction*

$$Q_1, Q_2, Q_3, \cdots, Q$$

   of Q from a collection of assumptions which includes the statement P.

***4. Rule of Generalization:
   Let $P(x)$ denote any statement which contains at least one occurrence of the variable x. *We may infer the general statement $\forall x,\ P(x)$ from any deduction*

$$Q_1, Q_2, Q_3, \cdots, P(x)$$

   of the statement $P(x)$ from any collection of assumptions, provided that the variable x does not occur in any of the assumption-statements.

Notes: *We assume that the two lists $x, y, \cdots, z$ and $\alpha, \beta, \cdots, \gamma$ are of the same length, and that all the variables in the list $x, y, \cdots, z$ are different. However, some of the expressions in the list $\alpha, \beta, \cdots, \gamma$ may occur more than once in the list $\alpha, \beta, \cdots, \gamma$.

**An application of the rule of inference for deductions as described above leads to a longer deduction

$$Q_1, Q_2, Q_3, \cdots, Q, P \Rightarrow Q.$$

This last deduction is regarded as a deduction of the statement $P \Rightarrow Q$ from all the original assumptions *except* P. For this reason, such an application of the rule of inference for deductions is often referred to as "discharging the assumption P."

(cont'd on page 6)

Figure 4 (cont'd)

RULES OF INFERENCE

Notes: **If P' is another one of the assumptions used in the deduction $Q_1, Q_2, Q_3, \cdots, Q$, then we may discharge P' from the deduction $Q_1, Q_2, Q_3, \cdots, Q, P \Rightarrow Q$ to obtain the still longer deduction $Q_1, Q_2, Q_3, \cdots, Q, P \Rightarrow Q, P' \Rightarrow (P \Rightarrow Q)$.

The latter is a deduction of $P' \Rightarrow (P \Rightarrow Q)$ from all the original assumptions except P, P'. One may continue in this way until all the assumptions are discharged. For example, if P, P', P'' are the only assumptions occurring in the deduction $Q_1, Q_2, Q_3, \cdots, Q$, then the deduction $Q_1, Q_2, Q_3, \cdots, Q, P \Rightarrow Q, P' \Rightarrow (P \Rightarrow Q), P'' \Rightarrow (P' \Rightarrow (P \Rightarrow Q))$ is a *proof* of the statement $P'' \Rightarrow (P' \Rightarrow (P \Rightarrow Q))$ from *no* assumptions.

If one desires to continue deductions beyond the discharging-of-assumptions stage, the definition of deduction must be complicated to prohibit making inferences from previous stages which depended on the assumptions.

***The rule of generalization does not discharge (or add) any assumptions. In other words, the deduction $Q_1, \cdots, Q, P(x), \forall x\, P(x)$ depends on exactly the same assumptions as does the deduction $Q_1, \cdots, Q, P(x)$.

Figure 5

A TYPICAL DEDUCTION

Q_1: $\forall x, 2x+5=9 \Rightarrow 2x=4$	"known truth"
Q_2: $2x+5=9 \Rightarrow 2x=4$	Q_1, rule of inference for general statements
Q_3: $2x+5=9$	temporary assumption P
Q_4: $2x=4$	Q_2, Q_3, rule of inference for conditional statements
Q_5: $\forall x, 2x=4 \Rightarrow x=2$	"known truth"
Q_6: $2x=4 \Rightarrow x=2$	Q_5, rule of inference for general statements
Q: $x=2$	Q_6, Q_4, rule of inference for conditional statements
$P(x)$: $2x+5=9 \Rightarrow x=2$	$Q_1, \cdots, Q$, rule of inference for deductions
$\forall x, P(x)$: $\forall x, 2x+5=9 \Rightarrow x=2$	$P(x)$, rule of generalization

Figure 6

TAUTOLOGIES

1. **Truth Tables for Basic Statement Forms.**

P	Q	P *and* Q
t	t	t
t	f	f
f	t	f
f	f	f

P	Q	P *or* Q
t	t	t
t	f	t
f	t	t
f	f	f

P	*not* P
t	f
f	t

P	Q	$P \Rightarrow Q$
t	t	t
t	f	f
f	t	t
f	f	t

2. **Using the above tables one can construct truth tables for arbitrary statement forms, e.g.**

P	Q	*not* P	Q *or* (*not* P)
t	t	f	t
t	f	f	f
f	t	t	t
f	f	t	t

P	Q	*not* Q	*not* P	(*not* Q) $\Rightarrow$ (*not* P)	$P \Rightarrow Q$	$[($*not* $Q) \Rightarrow ($*not* $P)] \Rightarrow [P \Rightarrow Q]$
t	t	f	f	t	t	t
t	f	t	f	f	f	t
f	t	f	t	t	t	t
f	f	t	t	t	t	t

3. **A statement which results from the application (to arbitrary statements) of a statement form whose truth table has only t's in the last column is called a tautology; e.g. as the table above shows, if P, Q are *any* statements, then $[($*not* $Q) \Rightarrow ($*not* $P)] \Rightarrow [P \Rightarrow Q]$ is a tautology. The table below proves that $[(P \Rightarrow Q)$ *and* $(Q \Rightarrow R)] \Rightarrow [P \Rightarrow R]$ is a tautology (for any three statements P, Q, R.)**

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	$(P \Rightarrow Q)$ *and* $(Q \Rightarrow R)$	$P \Rightarrow R$	$[(P \Rightarrow Q)$ *and* $(Q \Rightarrow R)] \Rightarrow [P \Rightarrow R]$
t	t	t	t	t	t	t	t
t	t	f	t	f	f	f	t
t	f	t	f	t	f	t	t
t	f	f	f	t	f	f	t
f	t	t	t	t	t	t	t
f	t	f	t	f	f	t	t
f	f	t	t	t	t	t	t
f	f	f	t	t	t	t	t

Figure 7

AXIOMS

1. Axioms of Equality:

(Reflexive)	$\forall x,\ x=x$
(Symmetric)	$\forall x\ \forall y,\ x=y \Rightarrow y=x$
(Transitive)	$\forall x\ \forall y\ \forall z,\ x=y$ *and* $y=z \Rightarrow x=z$
(Additive)	$\forall x\ \forall y\ \forall z,\ x=y \Rightarrow x+z=y+z$
(Multiplicative)	$\forall x\ \forall y\ \forall z,\ x=y \Rightarrow zx=zy$

2. Commutative Axioms:

(Addition)	$\forall x\ \forall y,\ x+y=y+x$
(Multiplication)	$\forall x\ \forall y,\ xy=yx$

3. Associative Axioms:

(Addition)	$\forall x\ \forall y\ \forall z,\ x+(y+z)=(x+y)+z$
(Multiplication)	$\forall x\ \forall y\ \forall z,\ x(yz)=(xy)z$

4. Distributive Axiom:

$$\forall x\ \forall y\ \forall z,\ x(y+z)=xy+xz$$

5. Axioms of Zero and Unity:

(Zero)	$\forall x,\ x+0=x$
(Unity)	$\forall x,\ 1x=x$

6. Axioms of Negatives and Reciprocals:

(Negatives)	$\forall\ x,\ x+(-x)=0$
(Reciprocals)	$\forall x,\ x\neq 0 \Rightarrow x\left(\frac{1}{x}\right)=1$

7. $1\neq 0,\ 2\neq 0,\ 3\neq 0,\ 4\neq 0,\ \cdots$

Figure 8

TRUE STATEMENTS

1. Basic True Statements: Each axiom is a true statement and each tautology is a true statement (see Figures 6 and 7.)

2. Rules of Inference: A statement is true if it can be inferred from true statements by means of the rule of inference for conditional statements or the rule of inference for general statements. A statement is true if it results from applying the rule of generalization to a deduction which depends on no temporary assumptions, or from applying the rule of inference for deductions to a deduction which involves no temporary assumptions other than the one discharged by that application of the rule (see Figure 4.).

3. All true statements in the language of elementary algebra are obtained from axioms and tautologies by repeated use of the rules of inference as described in 2.

Note: Important true statements are called theorems (see Figure 9).

Figure 9

BASIC THEOREMS OF ELEMENTARY ALGEBRA

1. $a+x=a \Rightarrow x=0$
2. $a+x=0 \Rightarrow x=-a$
3. $0x=0$
4. $ax=a$ *and* $a\neq 0 \Rightarrow x=1$
5. $ax=1 \Rightarrow x=\frac{1}{a}$
6. $(-x)(-y)=xy$
7. $-x=(-1)x$
8. $-(x+y)=-x-y$
9. $-(x-y)=y-x$
10. $(x+y)^2=x^2+2xy+y^2$
11. $(x+y)(x-y)=x^2-y^2$
12. $(a+b)(x+y)=ax+bx+ay+by$
13. $xy=0 \Leftrightarrow x=0$ *or* $y=0$
14. $\frac{a}{b}=\frac{x}{y} \Leftrightarrow ay=bx$
15. $\frac{x}{y}=\frac{ax}{ay}$
16. $\frac{x}{z}+\frac{y}{z}=\frac{x+y}{z}$
17. $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$
18. $-\left(\frac{x}{y}\right)=\frac{-x}{y}$
19. $\frac{1}{xy}=\left(\frac{1}{x}\right)\left(\frac{1}{y}\right)$
20. $\left(\frac{a}{b}\right)\left(\frac{x}{y}\right)=\frac{ax}{by}$
21. $\frac{1}{\left(\frac{x}{y}\right)}=\frac{y}{x}$
22. $\frac{\left(\frac{x}{y}\right)}{\left(\frac{a}{b}\right)}=\frac{bx}{ay}$
23. $(xy)^n=x^ny^n$
24. $x^{n+m}=x^nx^m$
25. $x^{nm}=(x^n)^m$

Note: Theorems 1-12 as listed above are actually true statements in the language of elementary algebra; hence, by the appropriate applications of the rule of generalization (see Figure 4), each of them may be regarded as a general statement. The rule of inference for general statements may in turn be applied to substitute any expression for each occurrence of any variable in Theorems 1-12. Thus, each of these theorems may be viewed as shorthand for a great number of more complicated true statements. A similar remark applies to Theorems 13-22, except that the statements of these theorems as listed above are true only if no denominators are 0, e.g. $\frac{1}{xy}=\left(\frac{1}{x}\right)\left(\frac{1}{y}\right)$ should be regarded as an abbreviation for the conditional statement

$$x\neq 0 \textit{ and } y\neq 0 \Rightarrow \frac{1}{xy}=\left(\frac{1}{x}\right)\left(\frac{1}{y}\right).$$

Each of Theorems 23, 24, 25 is actually an infinite number of statements, true provided $x\neq 0$ and $y\neq 0$, e.g. the statement labeled Theorem 24 means that for any two integers n, m, the statement $\forall x,\ x\neq 0 \Rightarrow x^{n+m}=x^nx^m$ is provable in the language of elementary algebra.

Figure 10

THEOREM 6

Theorem: $(-x)(-y)=xy$

Proof:

1. $(-x)(-y)=(-x)(-y)+0$

2. $\quad =(-x)(-y)+0y$

3. $\quad =(-x)(-y)+[(-x)+x]y$

4. $\quad =(-x)(-y)+[(-x)y+xy]$

5. $\quad =[(-x)(-y)+(-x)y]+xy$

6. $\quad =(-x)[(-y)+y]+xy$

7. $\quad =(-x)0+xy$

8. $\quad =0+xy$

9. $\quad =xy$

10. $(-x)(-y)=xy$

Figure 11

THE INTEGERS

1. a. The positive integers are the numbers
$$1, 2, 3, 4, 5, \cdots .$$
   b. The sum of two positive integers is a positive integer and the product of two positive integers is a positive integer.
   *c. Obviously, any positive integer can be obtained by adding together sufficiently many 1's.

2. a. The integers are the numbers
$$\cdots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \cdots .$$
   The negative of a positive integer is called a negative integer.
   b. The product of two negative integers is a positive integer, and the product of a negative integer with a positive integer is a negative integer. This, together with Theorem 3 and 1b above, implies that the product of any two integers is an integer.
   c. The sum of two negative integers is a negative integer. This, together with 1b above, 3d below, and the axiom of zero, implies that the sum of any two integers is an integer.
   d. The negative of a negative integer is a positive integer; $-0=0$. Hence the negative of any integer is an integer.

3. a. If x, y are integers, then we say "y is greater than x" if an only if there exists a positive integer a such that $x+a=y$.
   *b. Obviously, given any two integers x, y, either x is greater than y, $x=y$, or y is greater than x.
   c. Any positive integer is greater than any negative integer.
   d. Suppose u is a negative integer and v is a positive integer. Then:
      If $-u$ is greater than v, then $u+v$ is a negative integer.
      If $-u=v$, then $u+v=0$.
      If v is greater than $-u$, then $u+v$ is a positive integer.

Note: *Although these two statements should be obvious, they cannot be proved in the language of elementary algebra. In fact, the notion of "integer" cannot be discussed *within* that language. Whenever we use integers in this course, we are either talking *about* the language of elementary algebra or about *models* for it.

An important fact which we use (in Chapter X) in talking *about* the language of elementary algebra (and which is closely related to 1c and 3b above) is the principle of *mathematical induction*: If $P_1, P_2, P_3, \cdots$ is an infinite list of statements, and if each of the infinite list of statements

$$\begin{gathered} P_1 \\ P_1 \Rightarrow P_2 \\ P_2 \Rightarrow P_3 \\ \vdots \end{gathered}$$

is known to be true, then we may infer that each of the statements $P_1, P_2, P_3, \cdots$ is true.

Figure 12

THEOREM 10

Theorem: $(x+y)^2=x^2+2xy+y^2$

Proof:

1. $(x+y)^2=(x+y)(x+y)$

2. $\quad =(x+y)x+(x+y)y$

3. $\quad =xx+yx+xy+yy$

4. $\quad =x^2+xy+xy+y^2$

5. $\quad =x^2+1xy+1xy+y^2$

6. $\quad =x^2+(1+1)xy+y^2$

7. $\quad =x^2+2xy+y^2$

8. $(x+y)^2=x^2+2xy+y^2$

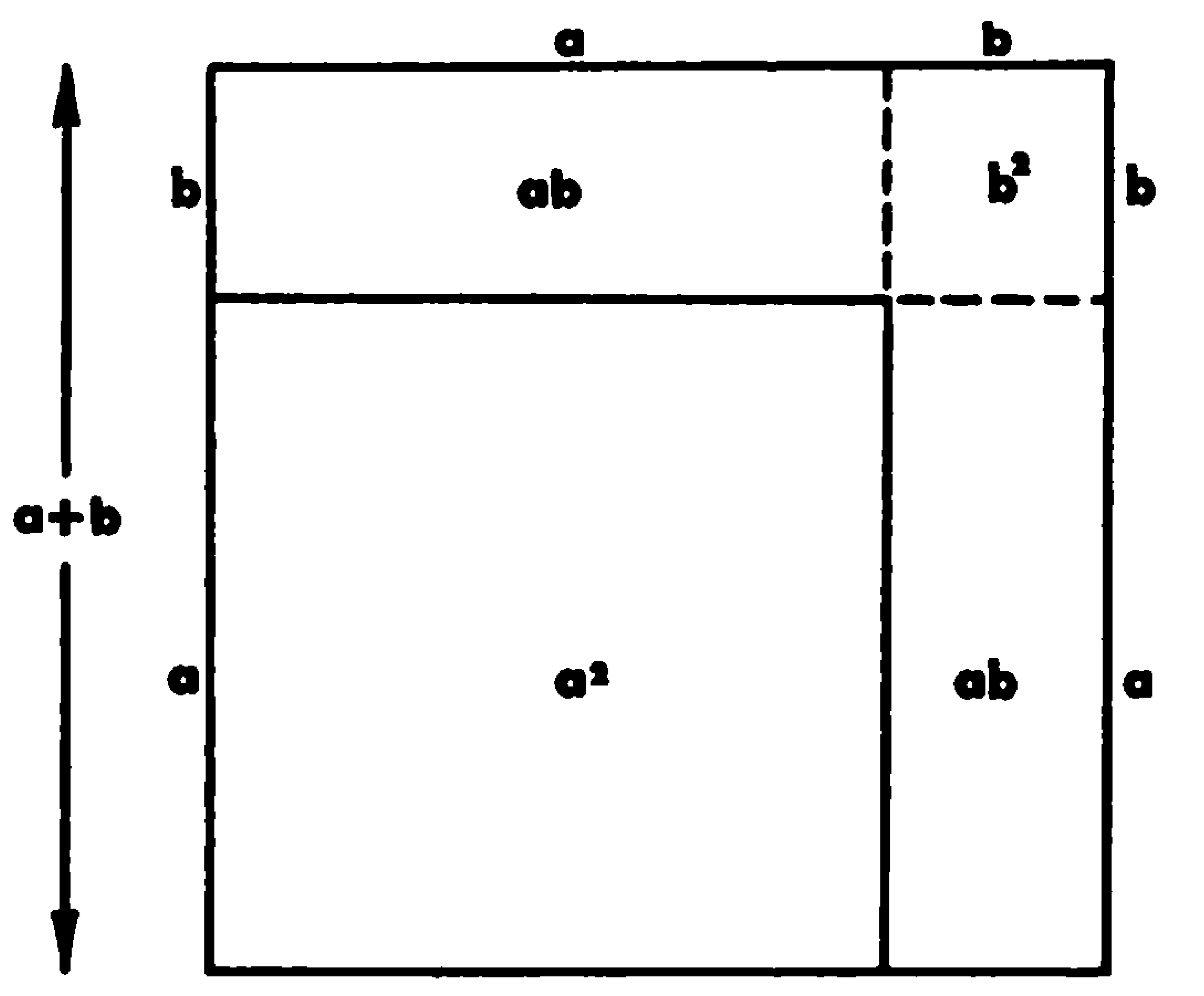


Figure 13

SOLUTION OF EQUATIONS

1. We say that the statement

$$\alpha=\beta$$

is an "equation in x" if at least one of the expressions α, β contains the variable x, and if all other variables in α, β are assigned fixed numerical values. We say that the variable a represents a *root* of the above equation in x if the statement

$$x=a \Rightarrow \alpha=\beta$$

is true. In other words, a root of such an equation is a number which when substituted for all occurrences of x in α, β makes the resulting equation true. To *solve* such an equation is to find the set of all its roots. The technique for solving an equation is usually as follows: We discover a list $a, b, c, \cdots, d$ of numbers for which we can prove the statement

$$\alpha=\beta \Rightarrow x=a \text{ or } x=b \text{ or } x=c \text{ or } \cdots \text{ or } x=d.$$

Then we can be sure that all roots of the equation are somewhere in the list $a, b, c, \cdots, d$. However we must then *check* each of the statements

$$\begin{gathered} x=a \Rightarrow \alpha=\beta \\ x=b \Rightarrow \alpha=\beta \\ x=c \Rightarrow \alpha=\beta \\ \vdots \\ x=d \Rightarrow \alpha=\beta \end{gathered}$$

to see which of the numbers in the list $a, b, c, \cdots, d$ actually are roots. We discard those that aren't and keep those that are. For example, if only the second and last of these statements turn out to be true, then we know that

$$\alpha=\beta \Leftrightarrow x=b \text{ or } x=d,$$

i.e., that the set of all roots of the equation $\alpha=\beta$ consists of the two numbers b, d.

2. Linear Equations: An equation in x is called *linear* if it is logically equivalent to an equation of the form

$$ax+b=0$$

where a, b represent fixed numbers. For linear equations we do not have to go through the procedure in 1 each time, because we have done it once and for all in Chapter XI, where we have shown that:

1) If $a=0$, then the equation above has no roots if $b\neq 0$, and any number is a root if $b=0$.
2) If $a\neq 0$, then

$$ax+b=0 \Leftrightarrow x=-\left(\frac{b}{a}\right).$$

3. Other classes of equations for which the procedure in 1 is carried out once and for all in Chapter XI are indicated in the statements below (see also Figure 15):

$$\begin{gathered} (x-a)(x-b)=0 \Leftrightarrow x=a \text{ or } x=b \\ (x-a)(x-b)(x-c)=0 \Leftrightarrow x=a \text{ or } x=b \text{ or } x=c \\ \text{etc.} \end{gathered}$$

Figure 14

MODELS FOR THE LANGUAGE OF ELEMENTARY ALGEBRA (FIELDS)

A system of numbers is said to be a *model* for the language of elementary algebra if and only if:

1. The sum and product of any two numbers in the system are again in the system.
2. The negative of any number in the system is again in the system.
3. The reciprocal of any non-zero number in the system is again in the system.
4. 0 and 1 are in the system.
5. All of the axioms (and therefore all of the theorems) of the language of elementary algebra are true when interpreted as statements about the system of numbers in question.

It is understood that, when discussing a particular model for the language of elementary algebra, we always interpret the symbols

$$\forall x$$

to mean "for every number x in the system which constitutes the model." For example, when discussing the system of rational numbers, these symbols may be conveniently read "for every rational number x."

We will use the word "field" to mean the same as "model for the language of elementary algebra."

Note: The prime example of a field is the system of *rational* numbers, which is defined to consist of all numbers which can be expressed in the form

$$\frac{a}{b}$$

where a is any integer and where b is any non-zero integer. It is clear that the system of rational numbers is a field (i.e. satisfies 1, 2, 3, 4, 5, above) and further, that any field must contain the field of rational numbers as a "subfield." Although there are many different fields, the only other examples which we consider in this course are the real numbers and the complex numbers (see Figures 18 and 20).

Figure 15

SOLUTION OF QUADRATIC EQUATIONS

Theorem. If $a \neq 0$, then
$$ax^2+bx+c=0 \Leftrightarrow (2ax+b)^2-(b^2-4ac)=0$$

Proof.
$$\begin{gathered} ax^2+bx+c=0 \\ \Updownarrow \\ 4a^2x^2+4abx+4ac=0 \\ \Updownarrow \\ 4a^2x^2+4abx+b^2=b^2-4ac \\ \Updownarrow \\ (2ax+b)^2=b^2-4ac \\ \Updownarrow \\ (2ax+b)^2-(b^2-4ac)=0 \end{gathered}$$

Theorem. If $a \neq 0$, then
$$\begin{gathered} (2ax+b)^2-(b^2-4ac)=0 \text{ and } y^2=b^2-4ac \\ \Updownarrow \\ x=\frac{-b+y}{2a} \text{ or } x=\frac{-b-y}{2a} \end{gathered}$$

Proof.
$$\begin{gathered} (2ax+b)^2-y^2=0 \\ \Updownarrow \\ (2ax+b-y)(2ax+b+y)=0 \\ \Updownarrow \\ 2ax+b-y=0 \text{ or } 2ax+b+y=0 \\ \Updownarrow \\ x=\frac{-b+y}{2a} \text{ or } x=\frac{-b-y}{2a} \end{gathered}$$

Note: Combining these two theorems we see that (under the hypothesis $a \neq 0$) if y represents a number whose square is b^2-4ac, then each of the numbers $\frac{-b+y}{2a}$, $\frac{-b-y}{2a}$ are roots of the equation $ax^2+bx+c=0$, and further, there are no other roots. It is customary to denote a number whose square is b^2-4ac by the symbol $\sqrt{b^2-4ac}$ if there is such a number. It is also customary to abbreviate the last line of the proof above to read $x=\frac{-b \pm y}{2a}$.

Thus we obtain the "quadratic formula": $ax^2+bx+c=0 \Leftrightarrow x=\frac{-b \pm \sqrt{b^2-4ac}}{2a}$.

This "formula" is true only under the two assumptions, $a \neq 0$, and the existence of a number whose square is b^2-4ac. As is explained in Chapters XVI and XVIII, this existence can always be guaranteed in the field of complex numbers and, if $b^2-4ac \geq 0$, in the field of real numbers. Of course there are two choices for $\sqrt{b^2-4ac}$ if there are any at all. However in the field of *real numbers* we are able to give a unique meaning to the symbol by choosing $\sqrt{b^2-4ac}$ to be the "positive" one of the two possibilities.

Figure 16

THE LANGUAGE OF ORDERED FIELDS

The *expressions* of the language of ordered fields are exactly the same as the expressions of the language of elementary algebra. (See Figures 1 and 2)

The *statements* of the language of ordered fields are constructed just as the statements of the language of elementary algebra are constructed, except that we allow as basic statements *both* equations

$$\alpha = \beta$$

and also inequalities

$$\alpha < \beta$$

where α, β are any two expressions. (See Figure 3)

The *rules of inference* for the language of ordered fields are exactly the same as the rules of inference for the language of elementary algebra. (See Figure 4)

The *axioms* of the language of ordered fields are the axioms 1-7 of the language of elementary algebra (see Figure 7) together with the following:

8. Axioms of Order

(Trichotomy)	$\forall x\ \forall y\ \forall z,\ [x<y \text{ or } x=y \text{ or } y<x]$ *and* $[x<y \text{ or } y<x \Leftrightarrow x \neq y]$ *and* $[x<y \Rightarrow \text{not } (y<x)]$
(Transitive)	$\forall x\ \forall y\ \forall z,\ x<y \text{ and } y<z \Rightarrow x<z$
(Additive)	$\forall x\ \forall y\ \forall z,\ x<y \Rightarrow x+z<y+z$
(Multiplicative)	$\forall x\ \forall y\ \forall z,\ x<y \text{ and } 0<z \Rightarrow zx<zy$
(Substitution)	$\forall x\ \forall y\ \forall u\ \forall v,\ x=u \text{ and } y=v \text{ and } x<y \Rightarrow u<v$

The *"true" statements* of the language of ordered fields are defined as in Figure 8, where "axiom" means any one of the axioms 1, 2, 3, 4, 5, 6, 7, 8.

Note: In the special case of rational numbers, we can *define* the meaning of $x<y$ as follows. First we define a rational number to be *positive* if and only if it can be represented as the quotient of two positive integers. Then, if x, y are any rational numbers, we say that $x<y$ is true if and only if the difference $y-x$ is a positive rational number. With this definition, we can show that the field of rational numbers satisfies all of the axioms 1, 2, 3, 4, 5, 6, 7, 8, i.e., that the field of rational numbers actually constitutes a model for the language of *ordered* fields.

Figure 17

SOME THEOREMS OF THE LANGUAGE OF ORDERED FIELDS

A. $x<y \Leftrightarrow y-x$ *is positive*

B. $x^2+y^2 \geqq 2xy$

C. $x \neq 0$ *and* $y \neq 0 \Rightarrow x^2+y^2>0$

D. $0<x<y \Rightarrow 0<\frac{1}{y}<\frac{1}{x}$

E. $x<y \Rightarrow x<\frac{x+y}{2}<y$

F. $|xy|=|x||y|$

G. $|x+y| \leqq |x|+|y|$

H $|x-a|<r \Leftrightarrow a-r<x<a+r$

Notes: 1. z *is positive* is an abbreviation for the statement $0<z$.

2. $y>x$ is an abbreviation for the statement $x<y$.
3. $x \leqq y$ is an abbreviation for the statement $x<y$ *or* $x=y$.
4. $x \geqq y$ is an abbreviation for the statement $y<x$ *or* $x=y$.
5. $a<b<c$ is an abbreviation for the statement $a<b$ *and* $b<c$.
6. Closely related to Theorem C is the fact that the square of any number in an ordered field is a non-negative number (here "x is non-negative" means $0=x$ *or* $0<x$).
7. $|x|$ means x if $0<x$, means 0 if $x=0$, and means $-x$ if $x<0$. Thus $|x|$ is always a non-negative number.
8. Since all of Theorems A-H are true statements in the language of ordered fields, we may invoke the rule of generalization and then the rule of inference for general statements to conclude that all these theorems remain true if any expression α is substituted for each occurrence of x and if any expression β is substituted for each occurrence of y.

Figure 18

REAL NUMBERS

1. The *Language of Real Numbers* is obtained by adjoining infinitely many axioms to the language of ordered fields. The statements which are to be adjoined as axioms are described as follows. Suppose $P(x)$ is any statement in the language of ordered fields which contains the variable x, but which does not contain the variables b, y, and which also does not contain the two symbols $\forall$, x in the particular combination $\forall x$. Then the statement below is an axiom for the language of real numbers.

   If the set (of real numbers) defined by $P(x)$ is non-empty and if there is a real number y such that y is an upper bound for the set defined by $P(x)$, then there is a real number b such that b is a least upper bound for the set defined by $P(x)$.

   One axiom for the language of real numbers is obtained for each statement $P(x)$ which satisfies the stated conditions. All the axioms obtained in this way are sometimes referred to collectively as the "least upper bound axiom." (It is the least upper bound axiom which makes calculus and other branches of analysis possible.) The English statement of the axiom above is to be regarded as an abbreviation for a rather complicated statement (in the language of ordered fields) whose parts are explained below.

   a) If $Q(y)$ is any statement, then *there is a y such that $Q(y)$* is an abbreviation for *not* [$\forall y$, *not* $Q(y)$].
   b) *The set defined by $P(x)$ is non-empty* is an abbreviation for *there is an x such that $P(x)$*.
   c) *y is an upper bound for the set defined by $P(x)$* is an abbreviation for $\forall x$, $(P(x) \Rightarrow x \leqq y)$.
   d) *b is a least upper bound for the set defined by $P(x)$* is an abbreviation for *b is an upper bound for the set defined by $P(x)$ and $\forall y$, if y is an upper bound for the set defined by $P(x)$, then $b \leqq y$.*

   It can be proved that a set has at most one least upper bound.

2. A *Model* for the language of real numbers can be constructed by taking a geometrical straight line and choosing two points on it to correspond to 0 and 1. The points on the line can then be considered as "numbers." That there is a unique geometrically natural way of defining the four algebraic operations for such "numbers" is sometimes proved in more advanced courses (addition is easier than multiplication). In this course we have located those points on the line which correspond to *rational* numbers. Note that although the rational numbers are contained as a subfield in the real numbers, the rational numbers do not constitute a model for the language of real numbers. The last assertion follows from our proof in Chapter XII that there is no rational number whose square is 2, together with the fact (discussed below) that any model for the language of real numbers contains a square root for *any* positive number (in particular for 2). It is customary to speak of *the* field of real numbers, even though we know that there are many different models for the language of real numbers. This custom is partly justified by the fact that all the models which we meet in everyday life for the language of real numbers are very much alike. By contrast, models for the language of elementary algebra can differ very essentially in certain of their properties; to see this one need only remember that the rational numbers, the real numbers, and the complex numbers are three quite different models for the same language.

(cont'd on the next page)

Figure 18 (Cont'd)

REAL NUMBERS

3. *The Action of Rational Exponents on Positive Real Numbers* is defined as follows. If a is a positive real number and if n is any non-zero integer, then $a^{\frac{1}{n}}$ is defined to be the least upper bound of the set defined by the statement $x^n \leq a$. It can then be proved that $a^{\frac{1}{n}}$ is a positive real number such that $(a^{\frac{1}{n}})^n = a$. If $\frac{m}{n}$ is any rational number, we define $a^{\frac{m}{n}}$ to be $(a^{\frac{1}{n}})^m$. It can then be shown that the definition of $a^{\frac{m}{n}}$ is independent of the representation $\frac{m}{n}$ chosen for the rational number, and that the laws of exponents

$$(ab)^r = a^r b^r$$
$$a^{r+s} = a^r a^s$$
$$a^{rs} = (a^r)^s$$

hold true if a, b represent positive real numbers and if r, s represent any rational numbers.

Figure 19

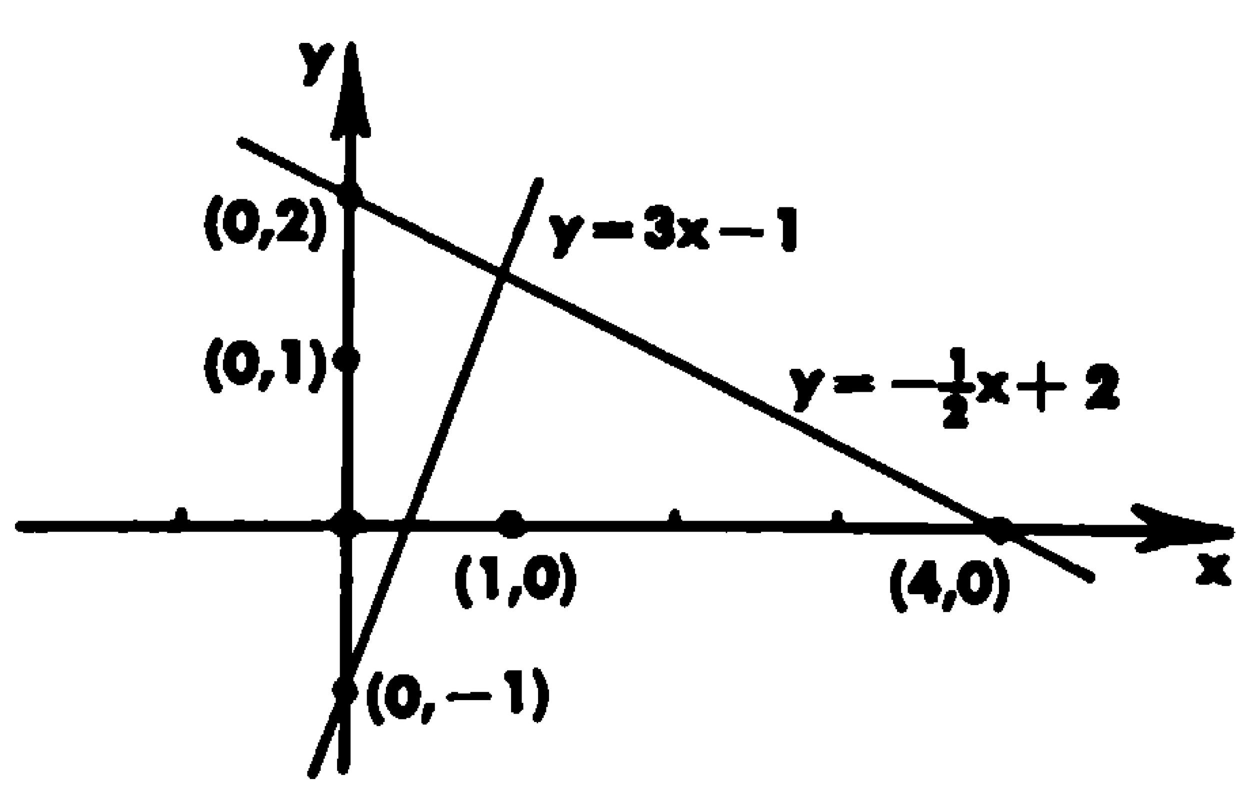
RELATIONS, GRAPHS, AND FUNCTIONS

1. A *relation in x, y* is a statement $R(x, y)$ in the language of ordered fields in which both of the variables x, y occur and in which the two combinations $\forall x$, $\forall y$ do not occur. For the discussion below, we assume that any other variables which may occur in $R(x, y)$ are regarded as representing *fixed* real numbers.

2. Having chosen two perpendicular straight lines in a plane, and having also chosen a point named $(1, 0)$ on one line and a point named $(0, 1)$ on the other line, then (provided neither of these points is the point of intersection) there is determined a unique geometrically natural way of setting up a one-to-one correspondence between the set of all points in the plane and the set of all ordered pairs of real numbers. Such a correspondence is usually referred to as a "co-ordinate system." Given a co-ordinate system and given a relation $R(x, y)$ we can then define the *graph* of the relation $R(x, y)$ (with respect to the given co-ordinate system) to be the set of all points in the plane corresponding to ordered pairs (x, y) for which the statement $R(x, y)$ is true.

3. A relation $R(x, y)$ is said to be a *function* if the statement
$$\forall x\ \forall y_1\ \forall y_2,\ [R(x, y_1) \text{ and } R(x, y_2) \Rightarrow y_1 = y_2]$$
is true.

4. If a, b, c represent fixed real numbers and if at least one of a, b does not represent the number 0, then the statement
$$ax+by=c$$
is a relation whose graph is a straight line. Conversely, any straight line in the plane is the graph of such a relation for appropriate choices of a, b, c. If $a=0$ then the graph is a horizontal line and if $b=0$ then the graph is a vertical line (the "horizontal" direction is determined by the line containing the two points $(0, 0)$ and $(1, 0)$). If $b \neq 0$ then the above relation is a function. If none of a, b, c are 0 then the graph of such a relation can be obtained very quickly by noting that the two points corresponding to $\left(0, \frac{c}{b}\right)$, $\left(\frac{c}{a}, 0\right)$ must be on the graph and then simply drawing the straight line determined by these two points. If $b \neq 0$ then the above relation is logically equivalent to (and hence has the same graph as) the equation $y = mx + b'$ where $m = -\left(\frac{a}{b}\right)$ is called the *slope* of the line and where $b' = \frac{c}{b}$ is called the *y-intercept*. The effect which these two numbers have on the position of the graph is illustrated below.



Note that these two lines intersect in the point corresponding to the ordered pair $(\frac{6}{7}, \frac{11}{7})$, a fact which can be obtained directly from the two equations.

Figure 20

THE FIELD OF COMPLEX NUMBERS

1. The field of complex numbers consists of all ordered pairs (x, y) of real numbers. The relevant definitions are

(Equality)	$(a, b)=(c, d) \Leftrightarrow a=c$ *and* $b=d$
(Addition)	$(a, b)+(c, d)=(a+c, b+d)$
(Multiplication)	$(a, b)(c, d)=(ac-bd, ad+bc)$

2. The above definitions require us to make the definitions

$$0=(0, 0)$$
$$1=(1, 0)$$
$$-(a, b)=(-a, -b)$$
$$\frac{1}{(a, b)}=\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) \text{ if } (a, b) \neq (0, 0)$$

3. Every complex number (a, b) can be written in the form

$$(a, b)=(a, 0)+(0, 1)(b, 0)$$

which we abbreviate to

$$(a, b)=a+ib$$

where

$$i=(0, 1)$$

4. Each of the complex numbers i, $-i$ is a root of the equation

$$z^2+1=0$$

That is, $i^2=(-i)^2=-1$. In particular,

$$\frac{1}{i}=-i$$

Note: It is proved in more advanced courses that given any string $a_{n-1}, a_{n-2}, \cdots, a_1, a_0$ of n complex numbers, there is a complex number z such that $z^n+a_{n-1}z^{n-1}+ \cdots +a_1z+a_0=0$.

Briefly, "any polynomial equation has a complex root." For this reason the complex numbers are said to constitute an *algebraically closed field.*