Sets and Functions [1]

1 Sets

A **set** is a collection of **elements**. The expression $p \in S$ means p is an element of the set S. A set may be defined in several ways: in ordinary English, *e.g.,* let A be the set of positive even integers; by listing its elements within braces, *e.g.,* let $A = \{2, 4, 6, 8, ...\}$; or by using "set builder" notation, *e.g.,* $A = \{n \in \mathbb{Z} \,|\, n > 0 \,\text{and}\, n \,\text{is even}\}$, read: A is the set of all integers n such that $n > 0$ and n is even ($\mathbb{Z}$ is the standard notation for the integers).

A set does not normally have an order. Thus $\{a, b\} = \{b, a\}$. An **ordered set** is a set together with an ordering. When we want to stress that a set has been endowed with an ordering we will use parenthesizes instead of braces[2]: (a, b) is an ordered set and is not equal to (b, a). Also $\{a, a\}$ is redundant and should be written as $\{a\}$. But (a, a) is not at all the same as (a).

The following notations are standard:

- $\phi = \{\}$, the empty set.
- $A \subset B$: read A is a subset of B, meaning, every element of A is an element of B. *Example:* $\{2, 5\} \subset \{1, 2, 3, 4, 5\}$.
- $A \cup B$: A union B, meaning, the set of all elements that are in A **or** in B. *Example:* $\{\$, *, !\} \cup \{\alpha, !, \star, 17\} = \{\$, *, !, \alpha, \star, 17\}$.
- $A \cap B$: read A intersection B, meaning, the set of all elements that are in A **and** in B. *Example:* $\{\$, *, !\} \cap \{\alpha, !, \star, 17\} = \{!\}$.
- $A - B$: read A minus B, meaning, the set of all elements of A that are not elements of B. *Example:* $\{\$, *, !\} - \{\alpha, !, \star, 17\} = \{\$, *\}$.
- $A \times B$: read A cross (product) B, meaning, the set of ordered pairs (a, b) where $a \in A$ and $b \in B$. Since there is a natural one-to-one correspondence between $(A \times B) \times C$ and $A \times (B \times C)$, $((a, b), c) \longleftrightarrow (a, (b, c))$, we shall ignore the distinction between them and use the notation $A \times B \times C$ for the set $\{(a, b, c) \,|\, a \in A, b \in B, \,\text{and}\, c \in C\}$.

[2] There are some expections where braces are used for ordered sets. This will come up in Section **??**.

Other multiple cross products are defined similarly. *Examples:* $\{1,3\} \times \{0,1,2\} = \{(1,0),(1,1),(1,2),(3,0),(3,1),(3,2)\}$. $\{*, \#\} \times \{\%\} = \{(*, \%), (\#, \%)\}$.

- $A^n = A \times \cdots \times A$, n times. *Example:* $\{2,3\}^3 = \{(2,2,2),(2,2,3),(2,3,2),(2,3,3),(3,2,2),(3,2,3),(3,3,2),(3,3,3)\}$.

Some standard sets are:

- $\mathbb{Z}$: the integers (most likely from the German *Zahl*)
- $\mathbb{Q}$: the rationals (quotients)
- $\mathbb{R}$: the reals
- $\mathbb{C}$: the complex numbers

Remark. The sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are normally given an ordering. Interestingly, $\mathbb{C}$ is not typically ordered.

Interval Notation:

$$\begin{array}{rclrcl} [a,b] & = & \{x \in \mathbb{R} \mid a \leq x \leq b\} & [a,\infty) & = & \{x \in \mathbb{R} \mid a \leq x\} \\ (a,b) & = & \{x \in \mathbb{R} \mid a < x < b\} & (a,\infty) & = & \{x \in \mathbb{R} \mid a < x\} \\ (a,b] & = & \{x \in \mathbb{R} \mid a < x \leq b\} & (-\infty,b] & = & \{x \in \mathbb{R} \mid x \leq b\} \\ [a,b) & = & \{x \in \mathbb{R} \mid a \leq x < b\} & (-\infty,b) & = & \{x \in \mathbb{R} \mid x < b\} \end{array}$$

Remark. The notation "(a,b)" is ambiguous; it could represent an interval or an ordered pair. One has to consider the context to understand the intended meaning. On behalf of mathematicians everywhere, I apologize for any in convenience this may cause.

Examples:

- $\{x \in \mathbb{R} \mid x \leq -\sqrt{7}\} \cup \{x \in \mathbb{R} \mid x \geq \sqrt{7}\}$ is the solution set for $x^2 - 7 \geq 0$.
- $\mathbb{R} - \{0\}$ is the natural domain of $1/x$.
- $\mathbb{R}^2$ is the plane. $\mathbb{R}^3$ is 3-dimensional space. $\mathbb{R}^4$ is 4-dimensional space. And so on.
- $\phi \subset A$, $\phi = A \cap \phi$, and $A = A \cup \phi$ are true statements for all sets A.

- $\{x \in \mathbb{R} \mid -2 \leq x < 5\} = [-2, 5) = [-2, 7] \cap (-10, 5)$.
- $S = [0, 1] \times [0, 1]$ is the *unit square* in the plane $\mathbb{R}^2$ with corners (0,0), (1,0), (0,1), and (1,1).

Problems:

1. Describe $[0, 1] \times [0, 2] \times [0, 3]$.
2. Simplify $((1, 3) \cap (2, 5)) \cup [3, 4)$.
3. Let $A = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 9\}$, $B = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 4\}$, and $C = \{(x, y) \in \mathbb{R}^2 \mid y \geq 0\}$. Graph $A - B$, $A \cap (\mathbb{R}^2 - B)$, $A \cap C$, and $A - C$.
4. Find the solution set in $\mathbb{R}^2$ of $\sin x \cos y = 0$.
5. Draw $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{R}$, and $((0, 1] \cup \{2, 3\}) \times ([-2, -1] \cup (2, 3))$ as subsets of $\mathbb{R}^2$.
6. Let A be a set. What is $A \times \phi$?
7. [Hard] Let A, B, and C be sets. Prove that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$. (You can draw pictures to "see" this, but you need to reason from the definitions to prove it.)

2 Functions

Intuitively, a function f from a set A to a set B assigns to each element of A one element of B. Formally, f is a subset of $A \times B$ such that for every $a \in A$ there is one and only one $b \in B$ with $(a, b) \in f$. We normally write $f : A \to B$, and express $(a, b) \in f$ by $b = f(a)$.

A function $f : A \to B$ is **onto** if for every $b \in B$ there is at least one $a \in A$ such that $(a, b) \in f$, *i.e.,* such that $f(a) = b$. A function $f : A \to B$ is **one-to-one** if for every $b \in B$ there is at most one $a \in A$ with $f(a) = b$.

Let $f : A \to B$, $A' \subset A$, and $B' \subset B$. Then we define,

- $f(A') = \{b \in B \mid b = f(a) \,\text{for at least one}\, a \in A'\}$ and is called the **image** of A' under f. We call $f(A)$ the **range** of f.
- $f^{-1}(b) = \{a \in A \mid b = f(a)\}$.

- $f^{-1}(B') = \{a \in A \,|\, a \in f^{-1}(b) \text{ for at least one } b \in B'\}$

If f is one-to-one and onto then $f^{-1}(b)$ always consists of a single element and we regard f^{-1} as a function from B to A. In this case we say f is **invertible**.

A **binary operation** is a function from the cross product of two sets to a third set. For example, the adding of two numbers is a binary operation from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$. So is multiplication. For any binary operation $f : A \times B \to C$, if $a_1 = a_2 \in A$ and $b \in B$ then $f(a_1, b) = f(a_2, b)$. For multiplication this means for real numbers a, b, and c, if $a = b$ then $ac = bc$. Note that we have written $f(a, b)$ instead of $f((a, b))$ since this shorthand is customary.

Example 1. Let $S = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit, \square, \bigcirc, \star\}$ and let $L = \{\alpha, \theta, \phi, \pi, \zeta\}$. Let $f : S \to L$ be defined as indicated by Figure 1. But what *is* f really? It is the set of arrows. But each arrow is a pictorial representative of an ordered pair. Thus $(\clubsuit, \alpha) \in f$ but $(\diamondsuit, \zeta) \notin f$. Or, equivalently, $f(\clubsuit) = \alpha$ while $f(\diamondsuit) \neq \zeta$. This function is not one-to-one since, for example, $f(\clubsuit) = f(\bigcirc)$. It is not onto since there is no $x \in S$ such that $f(x) = \zeta$, that is, for every $x \in S$, $(x, \zeta) \notin f$. Or, we could say ζ is not in the range of f.

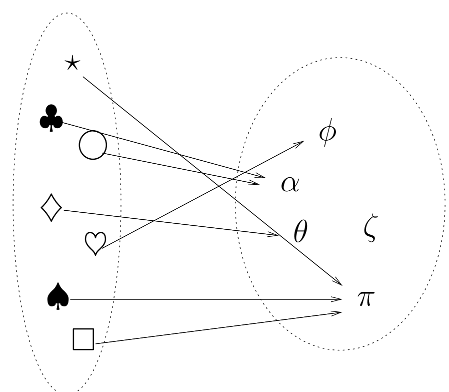

Figure 1: A function

If we order the elements of S and L then we can **graph** f. This is shown in Figure 2. We can see that the graph of f is a subset of $S \times L$. Notice that the familiar *horizontal line test* shows that f is not one-to-one, while the *vertical line test* confirms that f is indeed a function.

Additional Examples:

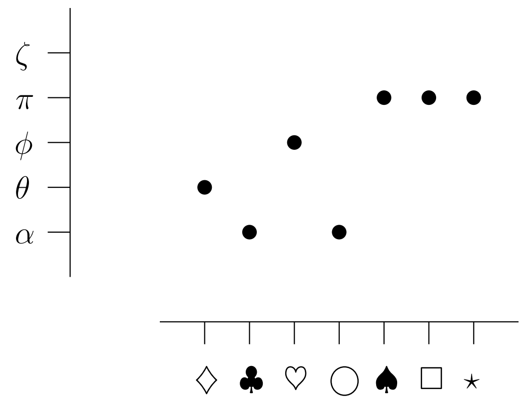

Figure 2: A graph of the function in Figure 1

1. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is the set $\{(x, y) \in \mathbb{R}^2 \,|\, y = x^2\}$. Thus, you can think of the function f as the graph in the plane $\mathbb{R}^2$.

2. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Then $f^{-1}(4) = \{-2, 2\}$, $f^{-1}([0, 1]) = [-1, 1]$, and $f^{-1}([1, 9]) = [-3, -1] \cup [1, 3]$.

3. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = \sin \pi x$. Then $f^{-1}(0) = \mathbb{Z}$, and
$$f^{-1}([0, 1]) = \cdots \cup [-4, -3] \cup [-2, -1] \cup [0, 1] \cup [2, 3] \cup \cdots$$

4. Let $A = \{1, 2, 3, ...\}$. Then the set $\{(1, 2), (2, 3), (3, 4), ...\} \subset A \times A$, is the function $f : A \to A$ produced by adding a one: $f(n) = n + 1$. It is one-to-one but not onto. But if we let $B = A - \{1\}$ and let $g : A \to B$ be addition by one, then g is onto.

5. Let $A = \{2, 3\}$. Let $f = \{(2, 3), (3, 3)\}$, $g = \{(2, 3), (3, 2)\}$, and $h = \{(2, 2), (2, 3)\}$. Then, f is a function from A to A that is not one-to-one or onto, g is a one-to-one onto function from A to A, while h is not a function. Check that $g^{-1}(f(3)) = 2$ and that $f(g(f(x))) = g(f(g(x)))$ for both $x \in A$.

Problems:

1. a. Solve $\log_2 \sin x = -\frac{1}{2}$.
   b. Let $h(x) = \log_2 \sin x$ for $x \in [0, \frac{\pi}{2}]$. Find an expression for the

inverse of h.
c. Suppose f and g are invertable functions and that $k = f \circ g$ is well defined. What is k^{-1}?

2. Let $f : \mathbb{R}^2 \to \mathbb{R}$ be defined by $f(x, y) = x^2 + y^2$. Draw a picture of $f^{-1}([4, 9])$. *Recall:* $[4, 9] \subset \mathbb{R}$ is the closed interval from 4 to 9. *Hint:* What is $f^{-1}(4)$?

3. Let $f : \mathbb{R}^2 \to \mathbb{R}$ be defined by $f(x, y) = \sin x \cos y$. Find $f^{-1}(0)$ and $f^{-1}(1)$. Draw pictures of them.

4. Let $f : \mathbb{R} \to \mathbb{R}^2$ be defined by $f(x) = (x, x^2)$. Show that f is one-to-one but not onto.

5. Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be defined by $f(x, y) = (x + y, x + y)$. Show that f is neither one-to-one nor onto. Describe the range of f.

6. Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be defined by $f(x, y) = (3x + 2y, x - y)$. Show that f is one-to-one and onto. Find f^{-1}. What is the image of $\{(x, y) \in \mathbb{R}^2 \,|\, x = y\}$?

The Axioms of Arithmetic[3]

Let's play a game. Let R be a nonempty set. A **binary operation** is a function from $R \times R$ to R. That is a binary operation takes two elements from R and outputs a single element of R. We shall suppose that we have two binary operations on R. The first is called *addition*. Given a and b in R addition gives an element $a + b$ in R. The other is called *multiplication*. Given a and b in R multiplication gives $a \cdot b \in R$. We shall assume that these two operations obey the axioms listed below. The game is to prove facts about R based solely on these axioms.

Axioms: For all a, b and c in R the following hold.

a. $a + b = b + a$ (addition is commutative)

b. $a + (b + c) = (a + b) + c$ (addition is associative)

c. There is an element $z \in R$,
independent of a,
such that $z + a = a$ (an additive identity exists)

d. There is an $\bar{a} \in R$, which depends on a, such that $\bar{a} + a = z$ (additive inverses exist)

e. $a \cdot b = b \cdot a$ (multiplication is commutative)

f. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (multiplication is associative)

g. There is an element $u \in R$, independent of a, such that $u \cdot a = a$ (a multiplicative identity exists)

h. If a is not an additive identity, there is an $\hat{a} \in R$, which depends on a, such that $\hat{a} \cdot a = u$ (multiplicative inverses exist)

i. $a \cdot (b + c) = a \cdot b + a \cdot c$ (multiplication distributes over addition)

Applications:

1. There is only one additive identity element in R. *Proof:* Suppose z_1 and z_2 are both additive identity elements. Then by (c) $z_1 + z_2 = z_2$ and $z_2 + z_1 = z_1$. But, by (a), $z_1 + z_2 = z_2 + z_1$. Thus, $z_1 = z_2$.

   We are now justified in saying that the "zero element" is unique and shall denote it by 0.

2. There is only one multiplicative identity element in R. *Proof:* **Problem 7**. The unique "unity element" shall be denoted by 1.

3. Additive inverses are unique. *Proof 1:* Let $a \in R$. Suppose $\bar{a}_1$ and $\bar{a}_2$ are additive inverses of a. Then $\bar{a}_1 = 0 + \bar{a}_1 = (\bar{a}_2 + a) + \bar{a}_1 = \bar{a}_2 + (a + \bar{a}_1) = \bar{a}_2 + (\bar{a}_1 + a) = \bar{a}_2 + 0 = \bar{a}_2$. The reader should check that each step used exactly one of the axioms. *Proof 2:* $a + \bar{a}_1 = 0 \Rightarrow \bar{a}_2 + (a + \bar{a}_1) = \bar{a}_2 + 0 \Rightarrow (\bar{a}_2 + a) + \bar{a}_1 = \bar{a}_2 \Rightarrow 0 + \bar{a}_1 = \bar{a}_2 \Rightarrow \bar{a}_1 = \bar{a}_2$. Note that we have used a basic property of all binary functions in adding $\bar{a}_2$ to both sides of an equation and have freely used more than one axiom per step.

4. Multiplicative inverses are unique. *Proof:* **Problem 8**.

5. Let $a \in R$. Then $a \cdot 0 = 0$. *Proof:* $a \cdot 0 = a \cdot 0 + 0 = a \cdot 0 + (a + \bar{a}) = (a \cdot 0 + a) + \bar{a} = (a \cdot 0 + a \cdot 1) + \bar{a} = a \cdot (0 + 1) + \bar{a} = a \cdot 1 + \bar{a} = a + \bar{a} = 0$. The reader should check each step to see which of the axioms are being applied.

6. Let $a \in R$. Then $\bar{\bar{a}} = a$. *Proof:* **Problem 9**. Hint: Start with $\bar{\bar{a}} = \bar{\bar{a}} + 0$.

7. Let $a \in R$. Then $\bar{a} = \bar{1} \cdot a$. *Proof:* Since additive inverses are unique we need only show that $a + \bar{1} \cdot a = 0$. $a + \bar{1} \cdot a = 1 \cdot a + \bar{1} \cdot a = a \cdot 1 + a \cdot \bar{1} = a \cdot (1 + \bar{1}) = a \cdot 0 = 0$. Notice the last step uses 5.

8. Let $a \in R - \{0\}$. Then $\hat{\hat{a}} = a$. *Proof:* **Problem 10**.

9. Let a and b be in R and suppose that $a \cdot b = 0$. Then either $a = 0$ or $b = 0$. *Proof:* **Problem 11**.

10. Let $a + c = b + c$. Then $a = b$. *Proof:* **Problem 12**.

11. **Problem 13**: Let $ac = bc$. Show that it need not follow that $a = b$.

If we let R be the real numbers $\mathbb{R}$ then the axioms apply to the normal addition and multiplication operations. It is customary to denote the additive inverse of a by $-a$ and its multiplicative inverse by a^{-1} or $1/a$, for $a \neq 0$.

Problem 14. Prove that $-1 \times -1 = 1$.

If we let R be rationals $\mathbb{Q}$, or the complex numbers $\mathbb{C}$, then the axioms still apply. This is clear for $\mathbb{Q}$. But for $\mathbb{C}$ it takes a bit of effort to show this. For the integers $\mathbb{Z}$ only axiom h fails to hold.

Problem 15. It is easy to check that $\mathbb{C}$ obeys axioms a through g and i. The only difficulty is axiom h. Let $a + ib \in \mathbb{C} - \{0\}$. Find $c + id \in \mathbb{C}$ such that $(a + ib)(c + id) = 1$, and thus establish axiom h. (It is to be understood that a, b, c and d are real numbers.)

Project 1. Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Define addition and multiplication as follows. Let $a \oplus b$ be the remainder of $a + b$ divided by n and let $a \otimes b$ the remainder of $a \times b$ divided by n. For example, in $\mathbb{Z}_7$ we get $5 \oplus 5 = 3$, because $10 \div 7$ has remainder 3; and $4 \otimes 5 = 6$, because $20 \div 7$ has remainder 6. The set $\mathbb{Z}_n$ is called the *integers modulo n* and the operations are referred to as *modular arithmetic*.

(a) Show that $\mathbb{Z}_n$ satisfies axioms a through g and i.

(b) Show that $\mathbb{Z}_7$ satisfies axiom h but that $\mathbb{Z}_6$ does not.

(c) Study various $\mathbb{Z}_n$. Under what conditions does $\mathbb{Z}_n$ satisfy axiom h?

Why do proofs? [4]

Many of you will find the concept of a proof difficult and frustrating. This is because (1) the concept is difficult, (2) the reason for doing proofs may not be clear to you, and (3) the public schools have watered down much of the mathematics curriculum.

Let's address (2) first.

Proofs are to mathematics what experiments are to science: the test of truth. But there is difference. Science is based on **inductive reasoning**, while mathematics is based on **deductive reasoning**. Scientists will repeat an experiment many times. The results may confirm a given hypothesis. But this does not prove the hypothesis since further testing may produce contrary evidence. Through many trails, careful measurements and statistical analysis scientists gradually form increasingly accurate models of the physical, biological, and more recently, the social and economic worlds.

Mathematics is a abstract science. It does not deal directly with the objects of the world. Mathematics deals with abstract structures: numbers, equations, sets, operations like multiplication and integration, and so on. Mathematics is useful because many of the models used in science are mathematical in nature. The logical structures within mathematics seem to mirror patterns in nature. No one fully understands why this is. But, insights gleamed from mathematical proofs develop thinking patterns that are useful in broader areas.

A second reason for doing mathematical proofs in frankly political. If university courses were taught on the basis that truth comes from authority then students would fail to incorporate democratic values. They would come to feel comfortable in authoritarian settings. There is a connection between the academic's push for critical thinking (asking why?, demanding proof!) and the citizen's demand for accountability from political and business leaders. The view of most employers is mixed. They value employees who can think of new ways of doing things, but are afraid of employees who challenge the boss' authority. (However, having employees who speak out may well be good for the economy as a whole!)

If you are still not convinced you are left with a conundrum: if you are willing to believe what your professor says on faith, then you have to accept that you should understand proofs because your professor says so.

Let's work through one of the proofs from the last section in greater detail. This will begin to address point (1) above. We will redo Application 5.

Claim. Let R be a nonempty set that obeys the axioms listed in Section **??**. Let $a \in R$, then $a \cdot 0 = 0$.

We will use the *two column format* for our proof:

STEP	REASON
Let $a \in R$	R is nonempty
$a \cdot 0 = 0 + a \cdot 0$	axiom c
$= (a + \bar{a}) + a \cdot 0$	axiom d
$= (\bar{a} + a) + a \cdot 0$	axiom a
$= \bar{a} + (a + a \cdot 0)$	axiom b
$= \bar{a} + (a \cdot 1 + a \cdot 0)$	axiom g
$= \bar{a} + a \cdot (1 + 0)$	axiom i
$= \bar{a} + a \cdot (0 + 1)$	axiom a
$= \bar{a} + a \cdot 1$	axiom c
$= \bar{a} + 1 \cdot a$	axiom e
$= \bar{a} + a$	axiom g
$= 0$	axiom d

It is not necessary to do each step separately. Here is a shorted version of the same proof:

STEP	REASON
Let $a \in R$	R is nonempty
$a \cdot 0 = 0 + a \cdot 0$	axiom c
$= (a + \bar{a}) + a \cdot 0$	axiom d
$= \bar{a} + (a + a \cdot 0)$	axioms a and b
$= \bar{a} + (a \cdot 1 + a \cdot 0)$	axiom g
$= \bar{a} + a \cdot (1 + 0)$	axiom i
$= \bar{a} + 1 \cdot a$	axioms a, c and e
$= 0$	axioms g and d

How many steps is it okay to combine? Your reader should be able to reconstruct a complete one-step-at-a-time proof from your proof. Indeed, mature writes rarely employ the two-column format and instead write in standard English. The main point is that each step has to be justified by an axiom, a hypothesis, a previously known result or a basic law of logic. If you are new to proofs it is best to stick with one-step-at-a-time proofs, at least for now.

The concept of an **axiom**, or rather of an **axiomatic framework**, may also be new to you. Mature branches of mathematics and logic are governed by a collections of basic assumptions or postulates called axioms. For the set of real numbers we have listed those that deal with arithmetic. There are others that deal with ordering properties, e.g., $a > b \Longrightarrow a + c > b + c$. And there are axioms that allow us to analyze notions convergence and continuity of real valued functions on the real line. The theory of sets is defined in terms of axioms, see for example *Axiomatic Theory of sets and Classes,* by Murray Eisenberg. This was forced on mathematicians because there appeared to be logical paradoxes early on in set theory. The point of axioms is to take mathematical thought and break it down in to its most basic units. These basic units can then be seen as building blocks which are combined in accordance with logic. This is what we mean by deductive reasoning. Because each step is simple, sometimes ridiculously so, the whole structure is sound. Unlike music, language, politics or religion, mathematical concepts are universal across all modern cultures. You might compare the axioms developed by mathematicians to the way chemists break down ordinary matter into atoms.

I first encountered axioms and sets in a middle-class public school in the 6th grade. Times have changed. The following project is an attempt to address point (3).

Project 2. Use the internet to look up the address of your high school. Write a letter to the principal outlining how the education you received there has helped or hindered your progress in college.

> [Some] think that truth is only what sounds nice. If truth should prove to be something statistical, dry, or factual, something difficult to find and requiring study, they do not recognize it as truth; it does not intoxicate them. — Bertolt Brecht [1898–1956], German play-write.