SOLUTIONS TO EXERCISES FOR

MATHEMATICS 144 — Part 5

Fall 2006

V. Number systems and set theory

V.1 : The natural numbers and integers

Exercises to work

1. Follow the hint. If we multiply out the right side of the equation $x^2+bx+c = (x-r)(x-s)$ we see that $r + s = -b$ and $rs = c$, so both these quantities must be integers. It follows that $s = -b - r$ must also be a rational number. Furthermore, by the Quadratic Formula the roots r and s are given by

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

and hence we see that $r - s = \sqrt{b^2 - 4c}$, so that the right hand side must be a rational number.

In order to proceed we need the following variant of the proof that $\sqrt{2}$ is irrational: *If a positive integer m has a rational square root, then m is a perfect square.* PROOF : We might as well assume that $m > 1$ because we know that 1 is a perfect square. Express m as a product of powers of primes

$$m \quad = \quad p_1^{r_1} \;\cdots\; p_k^{r_k}$$

and write

$$m_1 \quad = \quad p_1^{s_1} \;\cdots\; p_k^{s_k}$$

where $s_j = 0$ if r_j is even and $s_j = 1$ if r_j is odd. Then $m = m_1 m_2$ where m_2 is a perfect square (it is the product of the numbers $p_j^{r_j - s_j}$, each of which is a perfect square because the exponents are all even) and m_1 is either 1 or a product of distinct primes. Clearly $\sqrt{m}$ is rational if and only if $\sqrt{m_1}$ is rational, so it suffices to show that the latter is true if and only if $m_1 = 1$, which holds if and only if each r_j is even. Assume the contrary, and suppose that p_j is a prime dividing m_1. If $\sqrt{m_1}$ is rational then we can write it as a quotient a/b where a and b are relatively prime positive integers. We then have $m_1 b^2 = a^2$, and since p_j divides m it follows that p_j must divide a^2, which in turn means that p_j^2 must also divide a^2; by our choice of a and b it follows that p_j does not divide b. But since p_j^2 does not divide m_1, this means that p_j must divide b, contradicting the previous sentence. It follows that $m_1 = 1$ and m is a perfect square.∎

By the preceding discussion, we have seen that $b^2 - 4c = d^2$ for some positive integer d. — CLAIM: If b is odd, then d is odd, and if b is even then m is even. — If b is odd, then b^2 is also odd, and hence $b^2 - 4c = d^2$ is odd, which means that m must also be odd. On the other hand, if b is even, then b^2 is divisible by 4, which means that $d^2 = b^2 - 4c$ is also divisible by 4, which in turn implies that d must be even.

We now have that

$$r \quad = \quad \frac{-b \pm d}{2}$$

where b and d are both even or both odd. In either case we know that $-b \pm d$ is even, and therefore it follows that r (and also s) must be an integer.■

ALTERNATE APPROACH. One might also try to prove this result by saying that if p/q is a rational root of the integral polynomial $F(t)$ then q divides the term of F with maximum degree and p divides the constant term; if the coefficient of the term of maximum degree is 1, then it follows that $q = \pm 1$ and hence the rational root must be an integer. These results on rational roots of integral polynomials follow from a fundamental result of C. F. Gauss on factoring polynomials with integer coefficients, but its proof is not covered in lower division mathematics courses, so we shall include a little background here. We know that $r = p/q$ is a rational root of a rational polynomial $F(t)$ if and only if $(t - r)$ divides $F(t)$. The result of Gauss states that if we can factor an integral polynomial $A(t)$ as a product of two rational polynomials $B(t)$ and $C(t)$ of lower degree, then in fact we can factor A as a product $B_1 C_1$, where B_1 and C_1 are integral polynomials that are rational multiples of B and C. Assuming that we have chosen p and q to have no nontrivial common factors, this means that $(qt - p)$ must divide $F(t)$ over the integers. But this means that the coefficient of the highest power of t in $F(t)$ must be divisible by q and the constant terms must be divisible by p.■

References for the factorization result are pages 297–298 of the book by Gallian listed below and pages 162–164 of the book by Hungerford listed below:

J. A. Gallian, *Contemporary Abstract Algebra* (Fifth Ed.), Houghton-Mifflen, Boston, 2002. ISBN: 0-6188-12214-1.

T. W. Hungerford, *Algebra* (Graduate Texts in Math. Vol. 73). Springer-Verlag, New York, 1974. ISBN: 0-387-90518-9.

2. DISREGARD. [In the proof above we use the fact that the square root of an integer is rational if and only if the integer is a perfect square, so any attempt to derive the irrationality of $\sqrt{2}$ from the preceding exercise is basically circular reasoning.]

3. Follow the hint. Let B be a nonempty set of A, and let C be the set of all integers of the form $n + b$ for some $b \in B$. Since B is nonempty, so is C. Also, $b \in B \subset A$ implies $b \geq -n$, and therefore $c = n + b \in C$ implies that $c \geq 0$. By the well ordering of the nonnegative integers we know that the (nonempty) set C has a least element m, and by the construction of C we know that $m - n \in B$. We claim it is the least element of B. Given $b \in B$ we know that $b + n \in C$, and by minimality of m se know that $m \leq n - b$; subtract n from both sides to conclude that $m - n \leq b$.■

V.2 : Finite induction and recursion

Exercises to work

1. Let $\mathbf{P}_k$ be the statement that $k^2 + 5k$ is even. Then $\mathbf{P}_0$ is true because the value of the $k^2 + 5k$ at $k = 0$ is zero, which is even. Suppose now that $\mathbf{P}_n$ is true; we then need to show that $(n+1)^2 + 5(n+1)$ is even. If we expand the latter we obtain

$$n^2 + 2n + 1 + 5n + 5 \quad = \quad (n^2 + 5n) + (2n + 6)$$

and by the induction hypothesis we know that $n^2 + 5n$ is even. However, we also know that $2n + 6$ is even, and therefore the displayed quantity is expressed as a sum of two even integers and hence must be even itself. Thus we have shown that for all n we have $\mathbf{P}_n \Longrightarrow \mathbf{P}_{n+1}$, and this means that the statement in the exercise is true for all nonnegative integers k.■

2. Let $\mathbf{P}_n$ be the statement of the exercise for the nonnegative integer n. Strictly speaking there are two parts to this, one of which is to prove the formula for $1 + \cdots + n$ and the other of which is to do the same for $1^3 + \cdots + n^3$. Both statements are trivially true if $n = 0$, and we need to show that if $\mathbf{P}_n$ is true then $\mathbf{P}_{n+1}$ is also true.

We begin with the simpler formula, where we have

$$1 + \cdots + n + (n+1) \quad = \quad \frac{n^2+n}{2} + (n+1) \quad = \quad \frac{n^2+3n+2}{2} \quad = \quad \frac{(n+1)(n+2)}{2}$$

which shows that the first part of $\mathbf{P}_{n+1}$ is true. In the other case we have

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

$$\frac{(n^4+2n^3+n^2)+(4n^3+12n^2+12n+4)}{4} \quad = \quad \frac{n^4+6n^3+13n^2+12n+4)}{4} \quad =$$

$$\frac{(n^2+2n+1)(n^2+4n+4)}{4} \quad = \quad \frac{(n+1)^2(n+2)^2}{4} \quad = \quad \left(\frac{(n+1)(n+2)}{2}\right)^2$$

thus completing the derivation of $\mathbf{P}_{n+1}$ from $\mathbf{P}_n$.■

3. If $n = 1$ the formula is true because $1! = 1 = 1^1$. Suppose now that we have $n! \leq n^n$ for some $n \geq 1$; we want to prove that $(n+1)! < (n+1)^{(n+1)}$. — Since $(n+1)! = n!(n+1)$, we must have

$$(n+1)! \quad = \quad n!(n+1) \quad \leq n^n(n+1) \quad < \quad (n+1)^n(n+1) \quad = \quad (n+1)^{(n+1)}$$

as required. To be more precise, let $\mathbf{P}_n$ be the compound statement in the exercise. Then the preceding shows that $\mathbf{P}_1$ implies $\mathbf{P}_2$, and our argument shows that if $\mathbf{P}_n$ is true for $n \geq 2$ then $n! \leq n^n$ implies $(n+1)! < (n+1)^{(n+1)}$, which is the conclusion of $\mathbf{P}_{n+1}$.

4. As noted in the hint, the cases $n = 1$ and $n \geq 2$ must be handled separately. For a sequence f of length one, we simply take $H(f) = 1$, while for sequences of length $n \geq 1$ we take $H(f) = f_{n-1} + f_{n-2}$.■

5. The crucial point is to understand how much of the payment of P units goes towards principal and how much towards interest. The interest owed at time n, which is computed using the balance after the previous payment at time $n-1$, is equal to $r\,x_{n-1}$, so this means that $P - r\,x_{n-1}$ goes to the principal and therefore we have

$$x_n \quad = \quad x_{n-1} \; - \; (P - r\,x_{n-1}) \quad = \quad (1+r)x_{n-1} \; - \; P\,.■$$

Although the problem does not ask for it, we shall also derive the formula for finding the value of P such that the loan will be paid off after M equal payments of P units. One can use the recursive relation to find an explicit formula for x_n in terms of L, r and P:

$$x_n \quad = \quad \frac{P}{r} \; + \; (1+r)\left[S - \frac{L}{r}\right]$$

The condition that x_M should equal zero leads to the following expression for P in terms of L, r and M:

$$P \quad = \quad \frac{rL(1+r)^M}{(1+r)^{M+1}-1}$$

If one intends to use this formula to work out a specific problem in computing payments, it is important to remember that the payments are usually monthly, so M denotes the number of months and r denotes the monthly interest rate (converted from a percentage to a decimal fraction, which means dividing the monthly percentage rate by 100).■

6. Following the hint, let $A = \{0\} \cup \sigma[\mathbf{N}]$. We need to show that $0 \in A$ and if $a \in A$ then $\sigma(a) \in A$. Then the third Peano axiom will imply that $A = \mathbf{N}$, and since A has only one element that is not the successor of anything else, the same must be true for $\mathbf{N}$.

The condition $0 \in A$ iis true by definition. If $a \in A$, then either $a = 0$ or $a = \sigma(b)$ for some $b \in \mathbf{N}$. In either case $\sigma(a) \in \sigma[\mathbf{N}] \subset A$, so this proves the second condition in the third Peano axiom.■

V.3 : Finite sets

Exercises to work

1. We prove this by induction on $|A|$. If $|A| = 1$, then $A = \{a\}$ for some a and the result is true by assumption (2). Suppose the result is true for finite sets with n elements and that $|A| = n+1$. Let $a \in A$ and set $A_0 = A - \{a\}$; let $C_0 = C \cap A_0 \times B$, and let $C' = C \cap \{a\} \times B$. We then have $C = C_0 \cup C'$ and $C_0 \cap C' = \emptyset$. Furthermore, assumption (2) implies that $|C'| = k$ and $|C_0| = |A_0| \cdot k$. Therefore we have

$$|C| \quad = \quad |C_0| \; + \; |C_1| \quad = \quad |A_0| \cdot k \; + \; k \quad =$$

$$(|A_0| + 1) \cdot k \quad = \quad |A| \cdot k$$

which completes the derivation of the inductive step.■

IMPORTANT GENERALIZATION.

One can view an ordered pair as a sequence of length 2; with this interpretation, the conclusion of the exercise extends to sequences of arbitrary finite length as follows:

> **Informal version.** *Suppose that we are given a sequence of k choices $\mathbf{ch}_i$ such that at each step the number n_i of alternatives does not depend upon the previous choices. Then the total number of possible choice sequences is $n_1 \cdot \; \ldots \; \cdot n_k$.*
>
> **Formal version.** *Let S be a set of sequences of length k whose terms lie in some finite set A, and for each i such that $1 \leq i \leq n$ let S_i be the set of all restrictions of sequences in S to $\{1, \;\cdots\;, i\}$; set $S_0 = \emptyset$. Suppose that for each i such that $0 \leq i < n$, and each $y \in S_i$ the number $N(y)$ of sequences $x \in S_{i+1}$ restricting to y is independent of y, and denote this number by n_{i+1}. Then the number $|S|$ of sequences in S is equal to the product $n_1 \;\cdots\; n_k$.*

This principle plays an important role in the proofs of many formulas (for example, showing that the number of permutations of $\{1, \cdots, n\}$ is $n!$ and the fact that the number of subsets of $\{1, \cdots, n\}$ with exactly r elements is equal to

$$\binom{n}{r} = \frac{n!}{(n-r)!\,r!} .$$

2. We can fit this example into the setting of the previous exercise with $A = B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. In this case the number $k = 5$, which is the number of integers that are odd if a is even and the number that are odd if k is odd. Therefore the total number of pairs in this case is equal to $10 \times 5 = 50$.■

3. By the theorem, there are as many Boolean subalgebras as there are partitions of $\{1, 2, 3, 4\}$ into disjoint subsets. The standard way to count partitions is to do so in decreasing order of the sizes of the subsets. We then have the following:

- There is one partition containing one subset of 4 elements.
- There are three partitions containing one subset of 3 elements and one of 1 element.
- There are three partitions containing two subsets of 2 elements.
- There are six partitions containing one subset of 2 elements and two of 1 element.
- There are four partitions containing four subsets of 1 element.

Thus the total number of partitions is $1 + 4 + 3 + 6 + 4 = 18$. Furthermore, the number with two atomic elements is the number of partitions into two subsets, which are all those of the second and third types. Thus there are exactly seven subalgebras that have precisely two atomic elements.■

V.4 : The real numbers

Exercises to work

1. Suppose that x_0 and x_1 are the two elements of the set S and they are indexed so that $x_0 < x_1$. We claim that x_1 is the least upper bound of S and x_0 is the greatest lower bound of S. The fiact that they are upper bounds follows because $y \in S$ implies $x_0 \leq y \leq x_1$. Suppose that U is another upper bound for S. Then $x_1 \in S$ implies that $x_1 \leq U$, which is precisely the condition for x_1 to be the least upper bound. Similarly, if L is a lower bound for S, then $L \leq x_0$, which is precisely the condition for x_0 to be the greatest lower bound for S.■

2. The least upper bound of $A \cup B$ is the larger of u and v. To prove this, let w be the larger of u and v. Then $x \in A \cup B$ implies $x \in A$ or $x \in B$, which in turn implies $x \leq u$ or $x \leq v$. In either case we have $x \leq w$, so w is an upper bound for $A \cup B$.

To see it is the least upper bound for $A \cup B$, suppose we have $z < x$; we need to show that z cannot be an upper bound for the union. Suppose that $w = u$. Then by the definition of least upper bound we know that there is some $a \in A$ such that $a > z$. Since z is not an upper bound for A it cannot be an upper bound for the larger set $A \cup B$. Likewise, if $z = v$ then there is some $b \in B$ such that $b > z$. Since z is not an upper bound for B it cannot be an upper bound for the larger set $A \cup B$. Therefore in either case we know that z cannot be an upper bound for $A \cup B$, and hence w must be a least upper bound for $A \cup B$.■

3. First of all, 0 is greater than every negative number, so 0 is an upper bound for A. Suppose now that $a < 0$. Then a cannot be an upper bound for A because we have $a < \frac{1}{2}a < 0$; thus if U is an upper bound for A then $U \geq 0$, and hence 0 must be the least upper bound for A.■

4. Since x is the least upper bound for A, we know that for each positive integer n the number $a - \frac{1}{n}$ is not an upper bound, and hence there is some $a_n \in A$ such that $a - \frac{1}{n} < a_n < a$. We claim $\lim_{n\to\infty} a_n = a$. Let $\varepsilon > 0$, and choose N such that $n \geq N$ implies $\frac{1}{n} < \varepsilon$. Then $n \geq N$ implies

$$a \;>\; a_n \;>\; a - \frac{1}{n} \;\geq a - \frac{1}{N} \;>\; a - \varepsilon$$

so that $|a_n - a| < \varepsilon$ as required.■

V.5 : Familiar properties of the real numbers

Exercises to work

1. There are many ways of doing this problem. For example, we can start by saying that there is a rational number r_0 such that $a < r_0 < b$ and another rational number r_1 such that $r_0 < r_1 < b$. An entire sequence of numbers r_n for $n > 1$ such that $r_n < \cdots < r_2 < r_1$ may be defined by setting

$$r_n \;=\; r_0 \;+\; \frac{r_1 - r_0}{n}$$

or alternatively one can take a sequence such that $a < r_0 < r_1 < r_2 < \cdots < r_n < \cdots < b$.■

2. Each case will be handled separately. It is probably worthwhile to begin by observing that we can write 1 in "base 16 decimal-like" notation as $0.\mathrm{FFFFFFF}..._{\mathbf{HEX}}$, because we have the following geometric series identity which works for all $n > 1$:

$$\sum_{k=1}^{\infty} \frac{n-1}{n} \cdot \left(\frac{1}{n}\right)^k \;=\; \frac{n-1}{n} \cdot \frac{1}{1-(1/n)} \;=\; 1$$

In the discussion below we shall always denote hexadecimal expansions by appending the subscript "$_{\mathbf{HEX}}$" as above; for example, $14_{\mathbf{HEX}}$ is equal to 20 (in base 10).

The easy cases. If k divides 16 evenly, then just as for decimals the expansion is given by $16/k$ in the first position and zeros afterwards, or equivalently by $(16/k) - 1$ in the first position and F's afterwards. Thus we have that $\frac{1}{2} = 0.800000..._{\mathbf{HEX}}$, $\frac{1}{4} = 0.400000..._{\mathbf{HEX}}$, and $\frac{1}{8} = 0.200000..._{\mathbf{HEX}}$.

The case $\frac{1}{3}$. The algorithm tells us exactly how to proceed. Start with $16 = x_1 \cdot 3 + y_1$, $16y_1 = x_2 \cdot 3 + y_2$, and so forth, obtaining $16 = 5 \cdot 3 + 1$, $16 = 16 \cdot 1 = 5 \cdot 3 + 1$, and similarly for every other value. The terms in the expansion are the x_j's, so this means that $\frac{1}{3} = 0.5555555555..._{\mathbf{HEX}}$.

The case $\frac{1}{5}$. In this case the algorithm yields $16 = 3 \cdot 5 + 1$, $16 = 16 \cdot 1 = 3 \cdot 5 + 1$, and similarly for every other value, so this means that $\frac{1}{5} = 0.3333333333..._{\mathbf{HEX}}$.

The case $\frac{1}{6}$. In this case the algorithm yields $16 = 2 \cdot 6 + 4$, $16 \cdot 4 = 64 = 10 \cdot 6 + 1$, and similarly for every other value, so this means that $\frac{1}{6} = 0.2\mathrm{AAAAAAAAA}..._{\mathbf{HEX}}$.

The case $\frac{1}{7}$. In this case the algorithm yields $16 = 2 \cdot 7 + 2$, $32 = 16 \cdot 2 = 4 \cdot 7 + 4$, $64 = 16 \cdot 4 = 9 \cdot 7 + 1$, $16 = 2 \cdot 7 + 2$, and one has a periodic pattern of length 3 for the remaining values, so this means that $\frac{1}{7} = 0.249249249249..._{\mathbf{HEX}}$.

The case $\frac{1}{9}$. In this case the algorithm yields $16 = 1 \cdot 9 + 7$, $112 = 16 \cdot 7 = 12 \cdot 9 + 4$, $64 = 16 \cdot 4 = 7 \cdot 9 + 1$, $16 = 1 \cdot 9 + 7$, and one has a periodic pattern of length 3 for the remaining values, so this means that $\frac{1}{9} = 0.1\mathrm{C}71\mathrm{C}71\mathrm{C}71\mathrm{C}7..._{\mathbf{HEX}}$.

The case $\frac{1}{10}$. In this case the algorithm yields $16 = 1 \cdot 10 + 6$, $16 \cdot 6 = 96 = 6 \cdot 10 + 6$, and similarly for every other value, so this means that $\frac{1}{10} = 0.1999999999..._{\mathbf{HEX}}$.

This completes the list of examples in the exercise, but of course one could continue to find hexadecimal expansions for all of the fractions $\frac{1}{k}$.■

3. The point of this exercise is that x has an eventually periodic decimal expansion if and only if $f(x)$ does.

Suppose that x is rational and that it has a decimal expansion that is eventually periodic with period p; in other words, there is some N such that for each $n \geq N$ the decimal digits x_n for x satisfy $x_n = x_{n+p}$. What can one say about the decimal digits y_n for $y = f(x)$ if $n \geq 2N$? If n is even then $y_n = 0$ and thus we trivially have $y_{n+2p} = 0 = y_n$, while if n is an odd number of the form $2m - 1$ then $2m - 1 \geq 2N$ implies $m \geq N$, so that $y_{2m-1} = x_m = x_{m+p} = y_{2p+2m-1}$. Thus the decimal expansion of $y = f(x)$ is eventually periodic, so that $f(x)$ is rational if x is rational.

Suppose now that $f(x)$ is rational. Since we know that $f(0) = 0$, we need only consider the case where $f(x)$ and x are both nonzero. — The conclusion is also trivial if $f(x)$ is a finite decimal fraction (in which case the same is true for x), so let us also assume that there are infinitely many decimal digits that are nonzero for x. Since only the odd entries are nonzero, it follows that the period of the tail end of the expansion must be even (this uses the fact that there are infinitely many nonzero terms so that there is a nonzero entry in the repeating part of the decimal exapansion). Thus if we let $y = f(x)$ as before, then we have some $2N$ and p such that $m \geq N$ implies $y_{2p+2m-1} = y_{2m-1}$. Thus for all m sufficiently large we also have $x_{m+p} = x_m$ as well.■

4. Follow the hints as usual. We want to apply the summation formulas

$$\sum_{i,j \geq 1} a_{i,j} \quad = \quad \sum_{i \geq 1} \sum_{j \geq 1} a_{i,j} \quad = \quad \sum_{j \geq 1} \sum_{i \geq 1} a_{i,j}$$

where $a_{i,j} = 2^{1-(i+j)}$ if $i \leq j$ and 0 otherwise. If we sum first over j holding i fixed and then sum over i, we find that the sum of this series is equal to the Swineshead series

$$\sum_{k \geq 1} \frac{k}{2^k}$$

as indicated in the problem. What happens if we sum over i holding j fixed and then sum over j? We obtain

$$\sum_{j \geq 1} \sum_{i \geq 1} 2^{1-(i+j)} \quad = \quad \sum_{j \geq 1} 2^{2-j} \quad = \quad 2$$

which is the value that Swineshead and Oresme computed in the 14th century.■