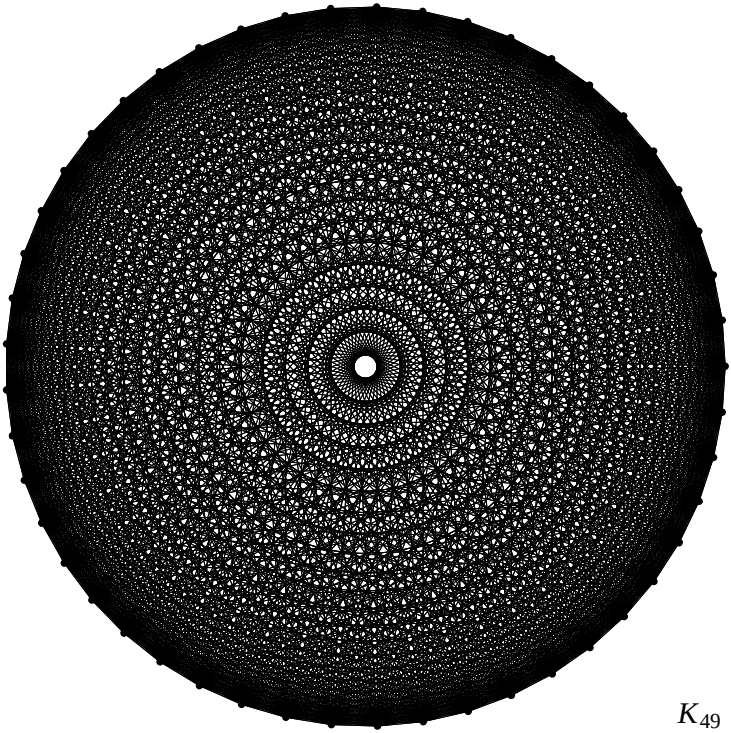
*

ISSN 1350-8539

M500

M500 213



K_{49}

The M500 Society and Officers

The M500 Society is a mathematical society for students, staff and friends of the Open University. By publishing M500 and 'MOUTHS', and by organizing residential weekends, the Society aims to promote a better understanding of mathematics, its applications and its teaching. Web address: www.m500.org.uk.

The magazine M500 is published by the M500 Society six times a year. It provides a forum for its readers' mathematical interests. Neither the editors nor the Open University necessarily agree with the contents.

MOUTHS is 'Mathematics Open University Telephone Help Scheme', a directory of M500 members who are willing to provide mathematical assistance to other members.

The September Weekend is a residential Friday to Sunday event held each September for revision and exam preparation. Details available from March onwards. Send s.a.e. to Jeremy Humphries, below.

The Winter Weekend is a residential Friday to Sunday event held each January for mathematical recreation. For details, send a stamped, addressed envelope to Diana Maxwell, below.

Advice to authors. We welcome contributions to M500 on virtually anything related to mathematics and at any level from trivia to serious research. Please send material for publication to Tony Forbes, above. We prefer an informal style and we usually edit articles for clarity and mathematical presentation. If you use a computer, please also send the file on a PC diskette or via e-mail.

Glenda Mary Franklin

Glenda died on 18 October 2006, aged 53, after a long illness.

She became involved with the running of M500 in 1990, and in 1993 she joined the Committee. From then until her death she was New Members Secretary and was responsible for all the mailings.

She held a BA (Hons) from the OU, and was a keen biker, helping administrate the AJS & Matchless Owners Club with 2000 members; she was also a motorbike riding instructor with the RAC for a time. She was a wild gardener, and Judith remembers Glenda's thoughtfulness in sending her a packet of seeds to plant after a meeting at Judith's house. She also enjoyed needlework and lace-making, puzzles, and was involved in her local community and church. She gave her time to HomeStart, a charity supporting families with young children, and for some years she produced the parish magazine. And of course she was fascinated by mathematics.

Donations in memory of Glenda can be given to St Laurence Bell Fund http://www.alvechurchbells.org.uk/ or The Salvation Army c/o Co-operative Funeral Services, Huxley House, 11 William Street, Redditch B97 4AJ (01527 66661).

Glenda is survived by her husband Geoff and her daughter and son-in-law Catherine and Andrew. She will be sadly missed.

Valuation rings: a worked example

Richard Williams

1 Introduction

This article documents my attempt to understand one aspect of a new public key encryption algorithm called *identity based encryption* [1]. A vital component of the algorithm is the group of *divisors* on an elliptic curve. I was completely stymied by this concept at first. It rapidly became clear that there was no obvious connection with the idea that, say, 2 divides 4, or even that $x+1$ divides x^2+2x+1; so I started to search for an explanation that I could understand. After a while I came across the following statement in [4, Chapter 2]: 'By a *prime divisor* we shall mean the maximal ideal P of some k-valuation ring of K.'

A valuation is a function which maps the elements of a field into a (usually additive) totally ordered semigroup. The simplest example is probably the absolute value of a real number. In this case the field is all the real numbers, and the semigroup is the positive reals. It is a semigroup because the positive real numbers have no inverses (i.e. negative real numbers) under addition. The subject of valuations and valuation rings is interesting in its own right because it is one of the areas where *analysis* and *algebra* overlap in a way which is non-trivial, but still straightforward enough to grasp from first principles.

For some time all my attempts to construct a valuation ring based on the definition in [4, p. 1] ran into a morass of inconsistencies. This is the 'worked example' I put together to test my (eventual) understanding. I have tried to show more stages of each derivation than seems to be common in many text books. Unfortunately this has made the paper rather long. For those not very familiar with abstract algebra I have added a very short section with some basic definitions. For a more complete treatment I'd recommend something like [5].

2 Absolute values

We start with the idea of an *absolute value*, a familiar concept from both real and complex analysis. Absolute values are defined on *rings* like the integers, $\mathbb{Z}$, but the definitions are equally applicable to *fields* like the real numbers, $\mathbb{R}$.

Somewhat lazily, I will use 0 and 1 for the additive and multiplicative identities, respectively, of all groups rings and fields. You should note, of course, that $\{0, 1\}$ in a field $\mathbb{K}$ is not necessarily the same as $\{0, 1\}$ in any other field.

2.1 Archimedean absolute values

Reference [2, p. 1] defines the abolute value on a ring R as follows:

A.1 $|x| \geq 0$, with equality if and only if $x = 0$;

A.2 $|x + y| \leq |x| + |y|$ (triangle inequality);

A.3 $|x \cdot y| = |x| \cdot |y|$.

This definition encapsulates the normal understanding of an absolute value. Unless R is trivial there must be at least one $x \in R$ such that $|x| \neq 0$. Suppose this value is α; then, by **A.3**, $|\alpha| = |1 \cdot \alpha| = |1| \cdot |\alpha|$, and hence we must also have $|1| \neq 0$. Moreover, since $|1| = |1 \cdot 1| = |1| \cdot |1|$ we must have $|1| = 1$. In general, if ζ is an nth root of unity, then $|\zeta^n| = |\zeta|^n = 1$ and so

$|\zeta| = 1$ and, in particular, $|-1| = 1$. **A.2** is also in accord with intuition. Taking R to be, for example, the integers, $\mathbb{Z}$, then $|x+y| = |x| + |y|$ if x, y have the same sign, and $|x+y| = ||x| - |y||$ if they are of different signs. It is easy to verify geometrically that $|z| = |x+iy| = \sqrt{x^2+y^2}$ over the complex numbers, $\mathbb{C}$, satisfies the conditions **A.1**–**A.3**.

2.2 Non-archimedean values

Suppose the triangle inequality condition is tightened as follows:

A.2′ $|x+y|_{\mathrm{n}} \leq \max(|x|_{\mathrm{n}}, |y|_{\mathrm{n}})$ (ultrametric inequality) [2, p. 3].

This is a stronger condition because

$$|x+y|_{\mathrm{n}} \leq \max(|x|_{\mathrm{n}}, |y|_{\mathrm{n}}) \leq |x|_{\mathrm{n}} + |y|_{\mathrm{n}}.$$

Thus it clearly defines an absolute value. An absolute value which satisfies **A.2′** is called *non-archimedean*. Any absolute value which satisfies **A.2** but not **A.2′** is *archimedean*.

The modified condition **A.2′** takes us away from the intuitive understanding of an absolute value. Is it possible to find an example of a non-archimedean absolute value over, say, the rationals, $\mathbb{Q}$? Suppose we write $x \in \mathbb{Q}$ as a *p-adic* number, $x = p^{\lambda} n/m$, where p is prime, λ is an integer and $\gcd(p,n) = \gcd(p,m) = \gcd(n,m) = 1$. Now define

$$|x|_{\mathrm{n}} = \begin{cases} 0, & x = 0, \\ p^{-\lambda}, & x \neq 0, \end{cases}$$

where p, λ are defined as above. Axiom **A.1** is satisfied since $|x| > 0$ for all $x \neq 0$. To see that **A.3** is satisfied, consider

$$|\alpha \cdot \beta|_{\mathrm{n}} = \left| p^a \frac{n_a}{m_a} \cdot p^b \frac{n_b}{m_b} \right|_{\mathrm{n}} = \left| p^{a+b} \frac{n}{m} \right|_{\mathrm{n}} = |\alpha|_{\mathrm{n}} \cdot |\beta|_{\mathrm{n}}.$$

Finally, if

$$|\alpha + \beta|_{\mathrm{n}} = \left| p^a \frac{n_a}{m_a} + p^b \frac{n_b}{m_b} \right|_{\mathrm{n}},$$

we can write

$$p^a \frac{n_a}{m_a} + p^b \frac{n_b}{m_b} = p^c \frac{n}{m},$$

assuming without loss of generality (and after considerable manipulation) that if $a \geq b$ then $c = (a-b) + k$, where k is an integer that satisfies $p^k | p^{a-b} n_a m_b + n_b m_a$. (The notation $x|y$ means 'x divides y'.) Inserting this into the definition of $|\ |_{\mathrm{n}}$ we arrive at

$$|\alpha + \beta|_{\mathrm{n}} = \left| p^c \frac{n}{m} \right|_{\mathrm{n}} = p^{-c} \leq \max(|\alpha|_{\mathrm{n}}, |\beta|_{\mathrm{n}})$$

and so **A.2′** is also satisfied.

2.3 Values in a finite field

An interesting consequence of the definitions **A.1**–**A.3** is the absolute value defined over any finite field. Let $\mathbb{F}$ be a finite field and $\mathbb{F}^\times$ be its multiplicative group, i.e. $\mathbb{F}^\times = \mathbb{F} - \{0\}$.

For any element $\xi \in \mathbb{F}^\times$ there is some integer, j, the *order* of ξ in $\mathbb{F}$ such that $\xi^j = 1$. This is easily seen. Suppose there is no such integer for some $\xi \neq 1$, and consider the sequence $X = \langle \xi^i | 1 \leq i \leq \#\mathbb{F} \rangle$. Then one of the following must hold.

1. For some n we have $\xi^i = \xi^n$ for all $i \geq n$. But this would mean that $\xi^{n+1} = \xi^n = \xi^n\xi$ and thus $\xi = 1$, which is a contradiction.
2. For some m, $m < n$, we have $\xi^{n+m} = \xi^n$. But in this case $\xi^{n+m} = \xi^n\xi^m = \xi^n$ and, hence, $\xi^m = 1$ which, again, is a contradiction.

Suppose $\xi \in \mathbb{F}^\times$ has order j. If we apply **A.3** then $|\xi^j| = |\xi|^j = 1$ and hence, for any $\alpha \in \mathbb{F}$,

$$|\alpha| = \begin{cases} 0, & \alpha = 0, \\ 1, & \alpha \neq 0, \end{cases}$$

which is known as the *trivial valuation*. This means, for example, that it is impossible to define a total order [6, p. 22] on a finite field using an absolute value because for any pair of general points $x, y \neq 0$ we have $|x| = |y|$, Notice that the trivial valuation is non-archimedean.

3 Exponential valuation functions

I shall use the definition of an exponential valuation from [2, p. 19]. Suppose $\mathbb{K}$ is a field and v a function $v : \mathbb{K} \to \mathbb{R} \cup \{\infty\}$ which satisfies

V.1 $v(x)$ is finite and real for all $x \neq 0$; $v(0) = \infty$;

V.2 $v(x + y) \geq \min(v(x), v(y))$;

V.3 $v(x \cdot y) = v(x) + v(y)$.

Then v is an *exponential valuation*. Note, to save a considerable amount of typing I shall write $\mathcal{R} = \mathbb{R} \cup \{\infty\}$. Remember that $\infty \notin \mathbb{R}$. (If it were, we would not need to call $1/0$ 'undefined'.)

Although these rules look somewhat strange, they are internally consistent. For example, if 0 is the additive identity element in $\mathbb{K}$ then **V.1** tells

us $v(0) = \infty$ and **V.2** gives $v(x) = v(x+0) \geq \min(v(x), \infty)$. Similarly, if 1 is the multiplicative identity, then **V.3** tells us that $v(x \cdot 1) = v(x) + v(1) = v(x)$ and so $v(1) = 0$. By a variant of the same argument used in section 2.1 we also get $v(\zeta) = 0$ for any ζ satisfying $\zeta^n = 1$. So, if $v(-1) = 0$ then, by **V.3**, $v(-x) = v(x)$. Also from **V.3** $0 = v(1) = v(x.(1/x)) = v(x) + v(1/x)$ and so $v(1/x) = -v(x)$. These simple identities, and others, are inherent in the definition of the exponential valuation, and are independent of the actual function chosen. For example, from **V.2** and **V.3**,

$$v\left(\frac{1}{2} + \frac{1}{2}\right) = v(1) = 0 > v\left(\frac{1}{2}\right).$$

But if $v(1/2) = 0$ then we just get a trivial valuation. If we assume that v is not trivial then, since $v(1/x) = -v(x)$, we get $v(2) > 0$, which of course is consistent with $v(1 + 1) = v(2) \geq v(1)$. Similarly we find that

$$v(4) = v(2 + 2) = v(2 \cdot 2) = 2v(2) \geq v(2).$$

Notice that although $v(2 + 1) \geq v(1)$ we don't know whether $v(3) \geq v(2)$.

Do such functions exist?

Suppose we have a non-archimedean absolute value, like the *p-adic* one for example. We could define

$$v\left(p^\lambda \frac{n}{m}\right) = -\log_p \left|p^\lambda \frac{n}{m}\right|_{\mathrm{n}} = \lambda.$$

V.1 and **V.3** are obviously satisfied in this definition. By **A.2′**

$$v(x + y) = -\log_p |x + y|_{\mathrm{n}} \geq -\log_p \max(|x|_{\mathrm{n}}, |y|_{\mathrm{n}}) = \min(v(x), v(y))$$

and so **V.2** is also satisfied.

3.1 Valuation rings

We can use the exponential valuation to define sets with interesting algebraic properties without any need to define a specific function. Let

$$\mathcal{O} = \{x \in \mathbb{K} \mid v(x) \geq 0\}.$$

We can show that $\mathcal{O}$ is a group under addition. Choose any $x, y \in \mathcal{O}$. By **V.2** $v(x + y) \geq \min(v(x), v(y)) \geq 0$ and so $x + y \in \mathcal{O}$. We already know that $0 \in \mathcal{O}$ and since $v(-x) = v(x)$ we also have $-x \in \mathcal{O}$. Since $\mathcal{O} \subseteq \mathbb{K}$ and addition in $\mathbb{K}$ is associative, the group properties are complete and $\mathcal{O}$ is an additive subgroup of $\mathbb{K}$.

Now consider multiplication. Let $\mathcal{O}_1 = \mathcal{O} - \{0\}$. For any $x, y \in \mathcal{O}_1$ we have, by **V.3**, $v(x \cdot y) = v(x) + v(y) \geq 0$ and so $(x \cdot y) \in \mathcal{O}_1$. We know that $v(1) = 0$ so the multiplicative identity is in $\mathcal{O}_1$. The associative property for multiplication is inherited from $\mathbb{K}$, but for a general element $x \in \mathcal{O}$ we have shown that $v(x) > 0 \implies v(1/x) < 0$ and so, in general, $x^{-1} \notin \mathcal{O}_1$.

The set $\mathcal{O}$, then, is a group under addition and a semigroup with identity under multiplication. This makes it a ring, known as the *valuation ring* of the valuation function v in $\mathbb{K}$.

Unlike my definition, [4, p. 1] starts by defining a valuation ring and uses this to define the exponential valuation: 'We say that ... $\mathcal{O} \subseteq \mathbb{K}$ is a valuation ring of $\mathbb{K}$ if $\mathcal{O} \neq \mathbb{K}$ and for every $x \in \mathbb{K}$ either x or x^{-1} lies in $\mathcal{O}$.' It was this definition, in particular, which caused me so much trouble when I started looking at this subject. Unless, for some x, elements x **and** x^{-1} lie in $\mathcal{O}$ it cannot easily be made an additive subgroup of $\mathbb{K}$. Based on **V.1**–**V.3**, however, we can restate Goldschmidt's definition like this:

$$\forall x \in \mathcal{O} \ \text{ either } \ v(x) = 0 \ \text{ or } \ x^{-1} \notin \mathcal{O}$$

and this, in turn, suggests yet another way to look at the relationship between $\mathbb{K}$ and $\mathcal{O}$. Consider the set $L = \{(a, b) \mid a, b \in \mathcal{O},\ b \neq 0\}$ with an equivalence relation $(a, b) \sim (c, d) \iff ad = bc$. If F is the resulting set of equivalence classes then we can define addition and multiplication operations on F as follows:

$$(a, b) \oplus (c, d) = (ad + bc, bd), \qquad (a, b) \otimes (c, d) = (ac, bd).$$

A quick examination shows that these are precisely the rules for the addition and multiplication of fractions; so, for any $(a, b) \in L$ we can treat it as a/b.

The identities for $\oplus$ and $\otimes$ are the equivalence classes $(0, 1)$ and $(1, 1)$, respectively, and the inverse elements of $(a, b),\ a \neq 0$ are $(-a, b)$ and (b, a). It can be verified that $(F, \oplus, \otimes)$ is a field. In fact, if we define the mapping

$$\phi : F \to \mathbb{K}, \ \text{where } \phi(a, b) = ab^{-1},$$

it can be seen that they are isomorphic. This is a feature of valuation rings: if $\mathcal{O}$ is a valuation ring in $\mathbb{K}$, then $\mathbb{K}$ is isomorphic to the *field of fractions* of $\mathcal{O}$.

3.2 The unit and value groups

You may have noticed, when we discussed whether $\mathcal{O}_1$ was a multiplicative group, that if $v(x) = 0$, then we have $x, x^{-1} \in \mathcal{O}_1$. We know that the valuation ring, $\mathcal{O}$, contains both 1 and -1, so it contains at least one

multiplicative subgroup. Consider the set $U = \{x \in \mathbb{K} \mid v(x) = 0\}$, which we know is not empty. Applying **V.3**, U must be closed under multiplication and for any $x \in U$, $0 = v(x) = v(x^{-1}) \in U$, so every element has a multiplicative inverse. Multiplication must be associative in U because it is in $\mathbb{K}$; so U is a multiplicative subgroup of $\mathcal{O}$. Moreover, since we have already seen that if $v(x) \neq 0$ then only one of x and x^{-1} is a member of $\mathcal{O}$, it must, therefore, be the largest multiplicative subgroup, known as the *group of units* of $\mathcal{O}$. Many references, including [4], designate this by the symbol $\mathcal{O}^\times$ to indicate that it is a subgroup. Note that $\mathcal{O}^\times \neq \mathcal{O} - \{0\}$.

So far it has been assumed that the range of a valuation, v, is a subset of $\mathcal{R}$ but this need not be the case. Define $\Gamma = \mathbb{K}^\times/\mathcal{O}^\times$, the quotient of $\mathbb{K}^\times$ over $\mathcal{O}^\times$ (see A.2). It turns out that Γ is isomorphic to the image $v(\mathbb{K}^\times)$.

It is incorrect to call $\mathcal{O}^\times$ the *kernel* (see A.2) of v because v is not a homomorphism. It is certainly not an ideal of $\mathcal{O}$ so we cannot directly apply the construction of section A.2, but we can still identify cosets.

Suppose $C_z = \{x \in \mathbb{K}^\times \mid v(x) = z\}$ remembering that, in general, $v(x) \in \mathcal{R}$ (unless v is a *discrete valuation*; see section 3.5). Now, if we apply **V.3**, we can define

$$\begin{aligned} C_r \oplus C_s &= \{x \in \mathbb{K}^\times \mid v(x) = v(x_r) + v(x_s),\, x_r \in C_r,\, x_s \in C_s\} \\ &= \{x \in \mathbb{K}^\times \mid x = x_r \cdot x_s,\, x_r \in C_r,\, x_s \in C_s\} = C_{r+s}. \end{aligned}$$

We see that $\mathcal{O}^\times = C_0$. Using **V.3**

$$\forall\, e \in C_0,\, x \in C_r \,:\, v(e \cdot x) = v(e) + v(x) = v(x)$$

and so $C_0 \oplus C_r = C_r \oplus C_0 = C_r$ which makes C_0 the identity element. For any coset C_r we can define

$$C_{-r} = \{x \in \mathbb{K}^\times \mid v(x^{-1}) = r\};$$

hence

$$C_{-r} \oplus C_r = \{x \in \mathbb{K}^\times \mid v(x) = 0\} = C_0$$

showing that every element has an inverse.

Taking $v(\mathbb{K}^\times)$ to be the image in $\mathcal{R}$ of $\mathbb{K}^\times$, then

$$\Gamma = \mathbb{K}^\times/\mathcal{O}^\times = \{C_z \mid z \in v(\mathbb{K}^\times)\}$$

is an abelian group which is the quotient of $\mathbb{K}^\times$ and $\mathcal{O}^\times$. From the definition of C_z it follows that the 'natural' mapping, ψ, of $v(\mathbb{K})$ to Γ given by $\psi(z) = C_z$ is an isomorphism.

If we write ζ for the natural mapping from $\mathbb{K}$ to Γ then $\mathbb{K}^\times$, $\mathcal{R}$ and Γ are related by

$$\mathbb{K}^\times \xrightarrow{v} v(\mathbb{K}^\times) \xrightarrow{\psi} \Gamma, \qquad v(\mathbb{K}^\times) \subseteq \mathcal{R}, \qquad \mathbb{K}^\times \xrightarrow{\zeta} \Gamma.$$

3.3 The maximal ideal of $\mathcal{O}$

Define $\mathcal{P} = \{x \in \mathbb{K} \mid v(x) > 0\} \cup \{0\}$. This set is an *ideal* of $\mathcal{O}$ (see section A.2) because (i) $0 \in \mathcal{P}$ and for any $r, s \in \mathcal{P}$, $r + s \in \mathcal{P}$; and (ii) for any $x \in \mathcal{O}$ and $p \in \mathcal{P}$ we have $xp \in \mathcal{P}$. The first condition is obtained from **V.1** and **V.2**, and the second from **V.3**. In fact, $\mathcal{P}$ is the *maximal ideal* in $\mathcal{O}$. A maximal ideal A of a ring R satisfies the following axioms:

M.1 A is an ideal of R and $A \neq R$;

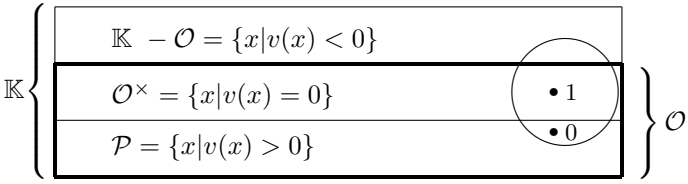
M.2 If $J \neq R$ is also an ideal of R and $A \subset J$ then $J = A$.

Thus $\mathcal{P}$ satisfies **M.1**. To see that it also satisfies **M.2**, suppose that there is an ideal J with $\mathcal{P} \subset J \subset \mathcal{O}$, where $\mathcal{P} \neq J \neq \mathcal{O}$. Now suppose that an element x belongs to $J - \mathcal{P}$. By the definition of $\mathcal{P}$ and $\mathcal{O}$, $v(x) = 0$ and, as we have already seen, this means that $x^{-1} \in \mathcal{O}$. So, applying the definition of an ideal, $x^{-1}x = 1 \in J$. Applying **I.3** from section A.2, $\forall x \in \mathcal{O}\ x = 1 \cdot x \in J$; so J contains every element of $\mathcal{O}$. Hence $1 \in J \implies J = \mathcal{O}$, which is a contradiction and so $\mathcal{P}$ is a maximal ideal.

3.4 k-valuations

Suppose $\mathbb{K}$ has a subfield k, and the multiplicative subgroup of k is $k^\times = k - \{0\}$. If v is defined in such a way that for any $x \in k^\times$, $v(x) = 0$, then v is called a *k-valuation*. It is not straightforward to construct a non-trivial k-valuation. The degree valuation on a field of rational functions (see section 4) is one example of a non-trivial *k-valuation*, where k is the base field of the functions ($\mathbb{Q}$).

The structures identified so far, $\mathcal{O} = \mathcal{O}^\times \cup \mathcal{P}$, are illustrated below.



The circle represents a subfield, k, of $\mathbb{K}$ if one exists. From the definition of v we know that $1 \in k \cap \mathcal{O}^\times$ and $0 \in k \cap \mathcal{P}$; v is a k-valuation iff $k \cap \mathcal{P} = \{0\}$ and $k \subset \mathcal{O}$.

3.5 Some analysis

Suppose we look at the image of the maximal ideal under v,

$$v(\mathcal{P}) = \{v(x) \in \mathcal{R} \mid x \in \mathbb{K} \text{ and } v(x) > 0\},$$

and ask whether this set has a lower bound distinct from 0. It turns out that if it does have a lower bound, say γ, and $x \in \mathbb{K}$ is chosen such that $v(x) = \gamma$, then v maps $\mathbb{K}$ only onto integer multiples of γ. To show this, let $y \in \mathbb{K}$ be such that $v(y) = \alpha v(x)$, where $1 < \alpha < 2$. Apply **V.3**:

$$v(y) - v(x) = v\left(\frac{y}{x}\right) = (\alpha - 1)\gamma = v(z).$$

But $0 < (\alpha - 1) < 1$; so there must be some z such that $v(z) < \gamma$, but this is a contradiction because γ is the lower bound of $v(\mathcal{P})$. Now suppose $2 < \alpha < 3$. From **V.3** we know that $v(x^2) = 2\gamma$ so we can repeat the argument:

$$v(y') - v(x^2) = v\left(\frac{y'}{x^2}\right) = (\alpha - 2)\gamma = v(z)$$

and so, again, we get a contradiction.

The conclusion must be, therefore, that if $v(\mathcal{P})$ has a lower bound, γ, then $v : \mathbb{K} \to \gamma\mathbb{Z}$, which is known as a *discrete* valuation, and induces the discrete topology [6, Chapter 7] on $\mathbb{K}$. On the other hand, if there is no lower bound in the image (if the set $v(\mathcal{P})$ is open), then the valuation is *dense* in $\mathcal{R}$. Given any two values, $x, y \in \mathbb{K}$ with $v(x) < v(y)$, we can always find a third, α, where $v(x) < v(\alpha) < v(y)$.

We have assumed, up to now, that relations such as $v(x) < v(y)$ are valid. Can we define the relation $<$ on the group Γ which we derived in section 3.2? Reference [4] proposes the following as a definition of the $\leq$ relation:

$$a\mathcal{O}^\times \leq b\mathcal{O}^\times \iff a^{-1}b \in \mathcal{O},$$

which does not, to me at least, seem particularly obvious.

First of all, what do we mean by $a\mathcal{O}^\times$? Well, applying the results we have derived so far, and remembering that $\mathcal{O}^\times = \{x \in \mathbb{K} \,|\, v(x) = 0\}$:

$$\begin{aligned} a\mathcal{O}^\times &= \{z \in \mathbb{K} \,|\, z = a \cdot x,\ x \in \mathcal{O}^\times\} \\ &= \{z \in \mathbb{K} \,|\, v(z) = v(a \cdot x) = v(a) + v(x) = v(a),\ x \in \mathcal{O}^\times\} \\ &= C_r, \end{aligned}$$

where $r = v(a)$. So we can restate the relation as $C_r \leq C_s \iff x_r^{-1}x_s \in \mathcal{O}$ for any x_r, x_s which satisfy $r = v(x_r)$ and $s = v(x_s)$. The first, and most obvious test to apply to this is the case $C_r = C_s$.

Suppose that $a, b \in C_r = \{x : v(x) = r\}$. In general $a \neq b$; so $a^{-1}b \neq 1$, but we can, however, say

$$v(a^{-1}b) = v(a^{-1}) + v(b) = v(b) - v(a) = 0.$$

So, in this case, $a^{-1}b \in \mathcal{O}^\times \subset \mathcal{O}$ and thus $a\mathcal{O}^\times \leq b\mathcal{O}^\times$. Similarly, since $v(b^{-1}a) = 0$, we also have $b\mathcal{O}^\times \leq a\mathcal{O}^\times$, and so $a\mathcal{O}^\times = b\mathcal{O}^\times = C_r$.

So far, so good. Now suppose $v(a) < v(b)$ (remember, we know that $\mathcal{R}$ is totally ordered and we are trying to show that Γ is). In this case

$$v(a^{-1}b) = v(b) - v(a) > 0;$$

so $v(a^{-1}b) \in \mathcal{O}$ but $v(b^{-1}a) \notin \mathcal{O}$. However, Γ is *totally ordered* [6, p. 22] if, for every C_r, $C_s \in \Gamma$, where $C_r \neq C_s$, then either $C_r < C_s$ or else $C_s < C_r$; and this is so here.

4 A discrete valuation

Finally, it's time to look at an explicit example of a valuation function. Let $\mathbb{K}$ be the field, $\mathbb{Q}(\xi)$, of rational functions in one variable over $\mathbb{Q}$ with the normal rules of addition and multiplication. In other words

$$\mathbb{K} = \left\{ \frac{g(\xi)}{h(\xi)} \mid h \neq 0,\ \gcd(g,h) = 1 \right\},$$

where g and h are polynomials. Define a function v on $\mathbb{K}$ as

$$v : \mathbb{K} \to \mathcal{R} \text{ where } v(g/h) = \begin{cases} \infty, & g = 0, \\ \deg(h) - \deg(g), & g \neq 0, \end{cases}$$

where, for example, $\deg(a_n\xi^n + \cdots + a_0) = n$. **V.1** is satisfied by definition. To show that **V.3** is satisfied consider

$$\begin{aligned} v\left(\frac{g_a}{h_a} \cdot \frac{g_b}{h_b}\right) &= \deg(h_a) + \deg(h_b) - \deg(g_a) - \deg(g_b) \\ &= (\deg(h_a) - \deg(g_a)) + (\deg(h_b) - \deg(g_b)) \\ &= v\left(\frac{g_a}{h_a}\right) + v\left(\frac{g_b}{h_b}\right). \end{aligned}$$

Finally, consider

$$v\left(\frac{g_a}{h_a} + \frac{g_b}{h_b}\right) = v\left(\frac{g_a h_b + g_b h_a}{h_a h_b}\right).$$

In the expression on the right hand side the numerator and denominator may now have a common factor, but we can assume that it is cancelled from both numerator and denominator without affecting v. Suppose

$$r(\xi) = g_a h_b = \sum_0^n r_i \xi^i \quad \text{and} \quad s(\xi) = g_b h_a = \sum_0^m s_i \xi^i.$$

So we get $\deg(g_a h_b + g_b h_a) \leq \max(m, n)$ with equality iff $n \neq m$ or else $r_n \neq -s_n$. Inserting this result into the definition of v we get

$$v\left(\frac{g_a}{h_a} + \frac{g_b}{h_b}\right) \geq \min\left(v\left(\frac{g_a}{h_a}\right), v\left(\frac{g_b}{h_b}\right)\right)$$

and so **V.2** is also satisfied.

4.1 The valuation ring

The algebraic structures created by this example are quite straightforward to construct.

The valuation ring, named $\mathcal{O}_d$ here for the *degree* valuation, is easily seen to be the set

$$\mathcal{O}_d = \left\{\frac{g(\xi)}{h(\xi)} \in \mathbb{K} \mid g, h \neq 0,\ \deg(h) \geq \deg(g)\right\} \cup \{0\}.$$

Notice that 0 has been included explicitly in $\mathcal{O}_d$ because $\deg h - \deg g$ is not well defined for this value. Also numerical elements, say $r/s \in \mathbb{Q}$, all belong to $\mathcal{O}_d$ because $\deg r = \deg s = 0$; so, immediately, $\mathbb{Q} \subset \mathcal{O}_d$.

Do we, in fact, find $\mathbb{K}$ as the field of fractions of $\mathcal{O}_d$? This is easy to verify. If we define

$$\begin{aligned}\mathcal{O}_d^{-1} &= \left\{\frac{g(\xi)}{h(\xi)} \in \mathbb{K} \,|\, g, h \neq 0,\ \deg(h) < \deg(g)\right\} \\ &= \{x \in \mathbb{K} \,|\, v(x) < 0\}\end{aligned}$$

then $\mathcal{O}_d^{-1} = \mathbb{K} - \mathcal{O}_d$. The field of fractions of $\mathcal{O}_d$ is the set $\{xy^{-1} | x, y \in \mathcal{O}_d\}$. For any element $z = xy^{-1}$, we get $v(z) = v(x) - v(y)$; so, if $v(x) \geq v(y)$ then $z \in \mathcal{O}_d$ and if $v(x) < v(y)$ then $z \in \mathcal{O}_d^{-1}$. Hence the field of fractions of $\mathcal{O}_d$ is $\mathcal{O}_d \cup \mathcal{O}_d^{-1} = \mathbb{K}$, as required.

4.2 The unit and value groups

The group of units of $\mathcal{O}_d$ is

$$\mathcal{O}_d^{\times} = \left\{\frac{g(\xi)}{h(\xi)} \in \mathcal{O}_d \mid \deg(h) = \deg(g)\right\}.$$

The multiplicative group, $\mathbb{Q}^{\times} = \mathbb{Q} - \{0\}$, of non-zero numerical fractions is wholly contained in the group of units $\mathbb{Q}^{\times} \subset \mathcal{O}_d^{\times}$ and, since $\mathbb{Q}$ is a subfield of $\mathbb{K}$ it follows that v is a $\mathbb{Q}$-valuation over $\mathbb{K}$.

One might be tempted to think that, since $\mathbb{Q}$ is a field, $\mathcal{O}_d^\times \cup \{0\}$ is as well. This is not the case. For $\mathcal{O}_d^\times \cup \{0\}$ is not closed under addition. Consider, for example,

$$a = \frac{1+\xi+\xi^2}{1+2\xi+\xi^2} \quad \text{and} \quad b = \frac{1-\xi-\xi^2}{1+2\xi+\xi^2}.$$

Both a and b are members of $\mathcal{O}_d^\times \cup \{0\}$, but their sum $a+b = 1/(1+2\xi+\xi^2)$ clearly is not.

The value group of $\mathbb{K}$ is the set of equivalence classes defined as $\mathbb{K}^\times/\mathcal{O}_d^\times = \Gamma = \{C_r\}$, where

$$C_r = \{x \cdot z \,|\, v(x) = r,\, z \in \mathcal{O}_d^\times\}.$$

Which, using the notation of section 3.5, we can write as $C_r = a\mathcal{O}_d^\times$, where a is any value satisfying $v(a) = r$. We can make this more explicit for the degree valuation:

$$C_r = \begin{cases} \{g/h \mid g,h \neq 0,\, \deg h - \deg g = r\}, & r \text{ finite,} \\ \{0\}, & \text{otherwise.} \end{cases}$$

It follows from this that Γ is countably infinite since there is a trivial one–one mapping from Γ to the integers $\mathbb{Z}$. The argument in section 3.5 that Γ is totally ordered was independent of $\mathbb{K}$ and v and so applies equally here.

For completeness we can write down the maximal ideal:

$$\mathcal{P}_d = \{g/h \in \mathbb{K} \,|\, g \neq 0,\, \deg h - \deg g > 0\} \cup \{0\}.$$

5 Where next? – Algebraic curves

This has taken me closer to understanding Goldschmidt's definition of a divisor, but where do elliptic curves come into it? Well, that will have to be a story for another day, but I think I can see a hint of the direction. In section 4 I looked at the field of fractions of polynomials in a single unknown, ξ. Suppose, instead, I look at polynomials in three unknowns: X, Y, Z and consider a set like

$$C = \left\{ (X : Y : Z) \mid \frac{Y^2Z - X^3 - Z^3}{Z^3} = 0 \right\}.$$

This is the elliptic curve $y^2 = x^3 + 1$ defined over the projective plane $\mathbb{P}^2$. (The $(X : Y : Z)$ notation is the normal representation of a point

in projective geometry.) It looks as though I can think about curves in a projective plane using the same mechanisms that I've used to consider valuation rings. For example, let $J = \{f \in \mathbb{K} \mid f(C) = \{0\}\}$, the set of all functions (as defined in section 4) which are zero everywhere on the curve C, where $\mathbb{K}$ in this case is the set of all rational functions over $\mathbb{P}^2$. This is an ideal of $\mathbb{K}$ (try it and see), but not a maximal ideal. Can I define a sequence of 'nested' ideals which terminate in a maximal ideal—and will this be a divisor?

There is more that can be said about the subject (much more), but this has, at least, explored some of the basic properties. I have followed the approach in [2]. For an alternative point of view, at least on section 2 see [5, Chapter IX]. This does not cover exponential valuations, but there are some interesting problems on non-archimedean absolute values.

A Some algebraic definitions

A.1 Groups, rings and fields

Some basic axiomatic definitions are given here. For more detail see, for example, [3] or [5]. Algebraic definitions all derive from the basic structure: a *group*. A group comprises a set of elements and a binary operator which, for the purposes of this definition, I shall write $\circ$. It doesn't much matter what the operator is because all we need to know is encapsulated in the mapping $\circ : G \times G \longrightarrow G$, where G is the set of elements. There are many formulations of the group axioms, but I shall use the following:

G.1 closure: $\forall x, y \in G \ : \ x \circ y \in G$;

G.2 identity element: $\exists e \in G \ \ \forall x \in G \ : \ e \circ x = x \circ e = x$;

G.3 inverse element: $\forall x \in G \ : \ \exists y \in G \ : \ x \circ y = y \circ x = e$;

G.4 associativity: $\forall x, y, z \in G \ : \ (x \circ y) \circ z = x \circ (y \circ z)$.

If **G.3** does not hold then G is known as a *semigroup*. If the group operation is *commutative*, in other words if $\forall\, x, y \ : \ x \circ y = y \circ x$, then the group is called *abelian*. We talk of G as 'a group under $\circ$', where $\circ$ is replaced by the operation we are interested in. This is sometimes written as $(G, \circ)$.

As an example, the set $G = \{0, 1, 2, 3, 4, 5\}$ is a group under addition modulo 6. Is the group $G - \{0\} = \{1, 2, 3, 4, 5\}$ a group or even a semigroup under multiplication modulo 6? [Hint: consider 2×3.]

Suppose a set R has two operations $\oplus$ and $\otimes$, which I will call 'addition' and 'multiplication' respectively. If R is a group under addition and $R - \{0\}$

is a semigroup under multiplication (and one other condition is met) then it is known as a *ring* and often written $(R, \oplus, \otimes)$. The axioms for a ring are:

R.1 $(R, \oplus)$ is a group;

R.2 $(R - \{0\}, \otimes)$ is a semigroup;

R.3 distributivity: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ and the corresponding relation holds for multiplication on the right-hand side.

We shall concentrate on rings where both operations are commutative. A ring where addition and multiplication are abelian groups is called a *field*.

A.2 Ideals and quotient groups

The set of integers, $\mathbb{Z}$, is a ring. Suppose we define a function, say ϕ, as $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}$, where $\phi(x) = x \pmod 5$. This function, ϕ, is an example of a *ring-homomorphism*:

RH.1 $\phi(x + y) = \phi(x) + \phi(y)$;

RH.2 $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$.

The image of ϕ is the set $\{0, 1, 2, 3, 4\}$. We can define the *kernel* of ϕ as $\ker \phi = \{x : \phi(x) = 0\}$.

The kernel of a ring homomorphism, such as ϕ, is an example of an *ideal*. An ideal I of a ring $(R, \oplus, \otimes)$ is a non-empty subset which satisfies the following axioms:

I.1 $I \subseteq R$;

I.2 $(I, \oplus)$ is a subgroup of R;

I.3 $\forall\, r \in R,\, n \in I \;:\; r \otimes n,\, n \otimes r \in I$.

Given that R is a ring, **I.2** may be more conveniently stated as

I.2a $0 \in I$;

I.2b $x, y \in I \implies x - y \in I$.

We have seen in the example above that $\ker \phi$ is a subgroup of $\mathbb{Z}$. We can define an equivalence relation (see A.3) $\sim$ on $\mathbb{Z}$ by $x \sim y \implies x - y \in \ker \phi$. The cosets of $\ker \phi$ are the equivalence classes under $\sim$. So, for example, we can write $C_n = \{x \;:\; x - n \in \ker \phi\}$. We can see that the number of equivalence classes corresponds to the size of the codomain of ϕ because, for example, $C_1 = C_6$.

If H is a subgroup of an abelian group G then the set of cosets of H is written G/H. In the running example, $\mathbb{Z}/\ker \phi = \{C_0, C_1, C_2, C_3, C_4\}$. The abelian group G/H is called the *quotient group*.

A.3 Miscellaneous definitions

A.3.1 Isomorphisms

Let A and B be rings (or fields of course) and ϕ be a function which maps elements of A to elements of B. If ϕ satisfies the properties

F.1 one–one: $\phi(x) = \phi(y) \iff x = y$;

F.2 linearity: $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$;

then ϕ is an *isomorphism*.

A.3.2 Equivalence relations and classes

A binary relation R on a set S is a subset of the set of ordered pairs of elements of S, $S \times S$. Typically, if $(x, y) \in R$ we write $x\,R\,y$. Thus, if $S = \mathbb{Z}$ and $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x < y\}$ then we can write $1 < 2 \iff 1\,R\,2$. A relation $\sim$ which satisfies the properties

E.1 symmetric: $a \sim b \iff b \sim a$,

E.2 transitive: $a \sim b$ and $b \sim c \iff a \sim c$,

E.3 reflexive: $a \sim a$

is called an *equivalence* relation.

Equivalence relations can be used to partition a set into *equivalence classes*. The equivalence class of an element x under the relation $\sim$ is the set $\{z | x \sim z\}$.

Given two equivalence classes R and S under the relation $\sim$ then either $R = S$ or $R \cap S = \emptyset$. The proof is trivial.

References

[1] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, *SIAM J. Computing* **32** No. 3, 586–615.

[2] P. M. Cohn, *Algebraic Numbers and Algebraic Functions*, Chapman & Hall, London 1991.

[3] P. M. Cohn, *An Introduction to Ring Theory*, Springer, New York 2000.

[4] D. Goldschmidt, *Algebraic Functions and Projective Curves*, Springer, New York 2002.

[5] S. Lang, *Undergraduate Algebra*, Springer, New York 2000.

[6] M. Searcóid, *Elements of Abstract Analysis*, Springer, New York 2002.

Emma Lehmer – 100 not out

Eddie Kent

Emma Markovna Trotskaia Lehmer (see http://www-history.mcs.st-and.ac.uk/PictDisplay/Lehmer_Emma.html) was born in Samara, Russia on 6 November 1906 to Motvey and Nadejda Trotsky. She got into Berkeley by a circuitous route, and there her favourite mathematics lecturer was Derrick Norman Lehmer. As well as taking several of his courses she did a research project with him on finding pseudosquares. It was at this time that she met his son Derrick ('Dick') Lehmer. In 1928 they married.

They received their B.A.s together and went to Brown to do a Masters, but Emma spent most of her time helping Dick, and typing his thesis, so he was able to go on for a Ph.D. while she was still working on her Master's Degree. This she received in 1930 for *A Numerical Function Applied to Cyclotomy*.

She never did a Ph.D. and so was barred from academia, but she didn't mind too much as the Lehmers wanted to work together and it was not possible for a husband and wife to lecture at the same institution. They moved from one place to another (these were the depression years) and she was always welcome in the mathematics faculties, and in their libraries, and a small bonus of not having a doctorate, in her own words, was that 'First of all there are lower expectations. If one happens to discover something new, one's peers are pleasantly surprised and generous in their praise. This is good for the morale ....'

They came to England, to Cambridge and Manchester, and met Hardy, Littlewood, Davenport, Erdös and others. Back in America for the war Emma was allowed to do a little teaching, and then Dick was recruited to help design and work on ENIAC. Some weekends the Lehmers used it to solve certain number theory problems using the sieve methods that they were working on, in particular to research Fermat's Last Theorem. Emma was pleased that ENIAC (when it was not broken down) could search a million or so numbers in only three minutes.

J. Brillhart in *Acta Arith.* **62** (1992), 207–213, writes about the Lehmers as a team. 'In the sixty years during which they collaborated, the Lehmers were a research team who personally influenced a large number of people with their knowledge, their courtesy and sociability, and their fine mathematical work. There is little doubt that one of their most enduring contributions to the world of mathematicians is their founding of the West Coast Number Theory Meeting [an annual event] in 1969.'

'Emma ... still goes each day, expectantly, to the mail box. Her address is still Miller Avenue, Berkeley CA 94708.'—Constance Reid.

So why not send her a card?

Problem 213.1 – Pascal triangle sums

Sebastian Hayes

Show that the sums of the reciprocals of the columns of Pascal's triangle, if they converge, are given by the simple formula

$$\sum_{n=1}^{\infty} \frac{k!(n-1)!}{(n+k-1)!} \;=\; \frac{k}{k-1}.$$

1										
1	1									
1	2	1								
1	3	3	1							
1	4	6	4	1						
1	5	10	10	5	1					
1	6	15	20	15	6	1				
1	7	21	35	35	21	7	1			
1	8	28	56	70	56	28	8	1		
1	9	36	84	126	126	84	36	9	1	
1	10	45	120	210	252	210	120	45	10	1

For example,

$$1+\frac{1}{3}+\frac{1}{6}+\frac{1}{10}+\cdots+\frac{2}{n(n+1)}+\ldots \;=\; 2.$$

$$1+\frac{1}{4}+\frac{1}{10}+\frac{1}{20}+\cdots+\frac{6}{n(n+1)(n+2)}+\ldots \;=\; \frac{3}{2}.$$

Problem 213.2 – e

Define a sequence $\epsilon_2, \epsilon_4, \epsilon_6, \ldots$ by

$$\epsilon_k \;=\; k+\frac{1+\epsilon_{k+2}}{1+2\epsilon_{k+2}}, \qquad \epsilon_\infty \;=\; 0.$$

Show that $e = 2 + \epsilon_2/(1+\epsilon_2)$.

If you have MATHEMATICA, you can easily verify the claim. Executing the following code (which assumes $\infty = 100$) produces 2.71828.

```
e[100] = 0;
e[k_] := e[k] = k + (1 + e[k + 2])/(1 + 2 e[k + 2]);
N[2 + e[2]/(1 + e[2])]
```

Solution 209.5 – Duelling lovers

A, B and C all love D and decide to fight a 3-way duel until only one survives. They draw lots to determine who will shoot first, second and third, and in the same sequence thereafter. They stand at the vertices of an equilateral triangle. The probability of each hitting his target on every shot is A: 0.9, B: 0.8, C: 0.7. What are their chances of survival if while all three are alive A and B shoot at each other and C shoots (i) at A, or (ii) in the air?

Norman Graham

Let the probabilities of killing with each shot be a (0.9), b (0.8) and c (0.7). Let the probabilities of missing be a' (0.1), b' (0.2) and c' (0.3). When only two are remainining (say A and B with A's turn to shoot), the probability of A surviving is

$$P_{\rm AB} \;=\; a + a'b'P_{\rm AB} \quad\Rightarrow\quad P_{\rm AB} \;=\; \frac{a}{1-a'b'} \;=\; 0.91837.$$

(i) The probabilities of A surviving for the sequences shown are as follows.

$$\begin{array}{lrcl} \text{ABC:} & P_1 &=& a\,c'P_{\rm AC} + a'b'c'P_1 \quad\Rightarrow\; P_1 \;=\; 0.252 \\ \text{CAB:} & P_2 &=& c'P_1 \quad\Rightarrow\; P_2 \;=\; 0.076 \\ \text{BCA:} & P_3 &=& b'P_2 \quad\Rightarrow\; P_3 \;=\; 0.015 \end{array}$$

The probabilities of C surviving are:

$$\begin{array}{lrcl} \text{ABC:} & P_4 &=& a\,P_{\rm CA} + a'bP_{\rm CB} + a'b'c\,b'P_{\rm CB} + a'b'c'P_4 \quad\Rightarrow\; P_4 \;=\; 0.715 \\ \text{CAB:} & P_5 &=& c\,b'P_{\rm CB} + c'P_4 \quad\Rightarrow\; P_5 \;=\; 0.319 \\ \text{BCA:} & P_6 &=& b\,P_{\rm CB} + b'P_5 \quad\Rightarrow\; P_6 \;=\; 0.066 \end{array}$$

Other probabilities are calculated in a similar manner.

(ii) The probabilities of A surviving (ignoring C while all three are alive) are:

$$\begin{array}{lrcl} \text{ABC, ACB or CAB:} & P_7 &=& P_{\rm AB}\,c'P_{\rm AC} \;=\; 0.256 \\ \text{BAC, BCA or CBA:} & P_8 &=& b'P_7 \;=\; 0.051 \end{array}$$

The full set of results (computing the average as one sixth of the sum) is given on the next page.

	Sequence	Prob. A survives	Prob. B survives	Prob. C survives
(i)	ABC	0.252	0.033	0.715
	ACB	0.252	0.066	0.682
	CAB	0.076	0.606	0.319
	BAC	0.050	0.217	0.732
	BCA	0.015	0.325	0.660
	CBA	0.015	0.661	0.324
	average	0.110	0.318	0.572
(ii)	ABC, ACB, CAB	0.256	0.021	0.724
	BAC, BCA, CBA	0.051	0.208	0.740
	average	0.153	0.115	0.732

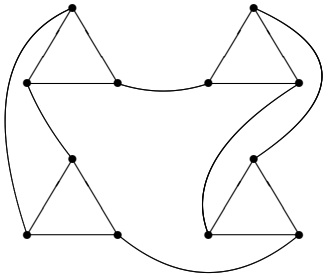
In summary, the worst shot (C) has the best chance of survival because he is not a target while all three are alive, and his chance improves further in (ii) because he then has the first shot after the first casualty. A's chance of survival is worse than B's in (i) because C first fires at A, but better in (ii) because the only shots are at each other.

Problem 213.3 – Triangles

Consider a graph T consisting of $2n$ separate triangles, $n \geq 1$. Now add $3n$ more edges such that (i) each new edge joins vertices of T belonging to two distinct triangles, and (ii) each vertex of T is adjacent to precisely one new edge. The result is a cubic graph, G_n, say.

For which values of n is G_n 3-edge-colourable?

For which values of n is G_n planar?



[A *graph* is one of those things you draw using vertices (points) and edges (lines joining pairs of points). *Planar* means you can draw it on paper without any lines crossing. *Cubic* means each vertex has three edges joined to it, and *3-edge-colourable* means that you can paint the edges of the graph with three colours such that the edges adjacent to a vertex have distinct colours.]

Problem 213.4 – Decimal continued fraction

Robin Whitty

Find an irrational number α whose decimal representation has the same digits as the terms in its continued fraction. Thus

$$\alpha = [\alpha_0; \alpha_1, \alpha_2, \alpha_3, \dots] \;=\; \alpha_0 \,.\, \alpha_1\alpha_2\alpha_3 \dots .$$

ADF writes — Start with $n = 0$ and $x = \alpha$. Then repeatedly apply the procedure $\alpha_n = \lfloor x \rfloor$, $x \to 1/(x - \lfloor x \rfloor)$ to get a sequence $[\alpha_0; \alpha_1, \alpha_2, \dots]$. For example, with $\alpha = e = 2.7182818284\dots$ you should obtain

$$[2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, \dots].$$

The expression $[\alpha_0; \alpha_1, \alpha_2, \alpha_3, \dots]$ generated in this way is called the *continued fraction* representation of α, and from its construction we see that

$$\alpha \;=\; [\alpha_0; \alpha_1, \alpha_2, \alpha_3, \dots] \;=\; \alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cfrac{1}{\alpha_3 + \ddots}}}.$$

The simplest continued fraction is $\phi = [1; 1, 1, 1, \dots]$. To compute its value observe that

$$\phi \;=\; 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}} \;=\; 1 + \frac{1}{\phi},$$

and hence $\phi = (\sqrt{5} + 1)/2$, the positive root of the quadratic $\phi^2 - \phi - 1$.

[If the problem as stated is too difficult, try it with binary representation instead of decimal.]

Problem 213.5 – Cubic

Show that the roots of

$$x^3 - 3\sqrt{3}x^2 - 3x + \sqrt{3} \;=\; 0$$

are $\tan 20°$, $\tan 80°$ and $\tan 140°$.

Japper-wok

Recall the Finnish poem, *Jäpperivokki* by Colin Davies [M500 **193**], which began thus.

Rillikki oli, ja lipiäset toopeet
Pyörivät ja kaksoisivat vaapeessa.
Ihan mimsiä olivat porokroopit
Ja muumiraatit rotkosesta pois.

Here it is again, translated into English by **Antti Rummukainen**.

Rillick was, lyeish fools
Spinning and twining in vaper.
Like mims were reindeerkroops
And Moomincouncils out of the gorge.

"Beware Japper-wok, my son!
Biting jaws, clawing nails!
Beware Jupjupbird and avoid
Ugly-like panther snatcher!"

He grabbed his Vorpaleish sword.
Looking for his Mankomied enemy for a long time
Therefore rested under Tumtumtree
And momentarily stood still thinking.

And in his inner thoughts
Japper-wok, with its flaming eyes,
Came quickly through the forest of Tulken
And welled up in its fire!

All of the sudden! All of the sudden! And straight through
Vorpal knife stabbed.
Left it dead, and along its head
He burned for the longest time.

"And have you killed the Japper-wok?
Come to my embrace my radiant son!"
Hey Rapjuice day! Kaluu! Kalei!
Giggled in joy.

Rillick was, lyeish fools
Spinning and twining in vaper.
Like mims were reindeerkroops
And Moomincouncils out of the gorge.

What's the next number?

Tony Forbes

Recall that sequence at the bottom of M500 **210** page 28. Bill Purvis added a few more terms to bring the total so far up to eleven:

1, 11, 21, 1211, 111221, 312211, 13112221, 1113213211, 31131211131221,

1321131123113112211, 11131221133112132113212221, ...

To get the $(n+1)$th entry you transform the nth entry by splitting it into blocks of repeated numbers and replacing each block $xx\ldots x$ with two numbers, nx, where n is the length of the block. For example, going from the 6th entry to the 7th, we have 312211 → 3 1 22 11 → 13 11 22 21 → 13112221.

The sequence is interesting. Since the construction method is reversible, it could be used as the basis of an efficient data compression algorithm were it not for its effect on single-digit blocks. Anyway, as a follow-up we suggest some things to investigate.

Do numbers other than 1, 2 and 3 ever occur?

Explain the rate of growth of the size of the terms. For $n = 1, 2, \ldots, 42$, the number of symbols in the nth term is given by

1, 2, 2, 4, 6, 6, 8, 10, 14, 20, 26, 34, 46, 62, 78, 102, 134, 176, 226, 302, 408, 528, 678, 904, 1182, 1540, 2012, 2606, 3410, 4462, 5808, 7586, 9898, 12884, 16774, 21890, 28528, 37158, 48410, 63138, 82350, 107312,

and apart from a few at the beginning they increase by a factor of about 1.3 at each stage.

Try different initial values.

Getting back to Diana Maxwell's interesting number sequence, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4 [M500 **207**], Eddie Kent suggested that the 18th number is 19 but he was unable to supply a proof [M500 **210**, p. 18]. Here I think I can help. Perhaps the most convincing argument is the existence of the unique polynomial of degree 17 that passes through $(1,4)$, $(2,4)$, $(3,4)$, ..., $(16,4)$, $(17,4)$ and $(18,19)$, namely

$$\frac{15}{17!}\,(x-1)(x-2)\ldots(x-17) \;+\; 4.$$

Hence the sequence is

$$\ldots, -266, -11, 4, 4, \ldots, 4, 4, 19, 274, 2569, 17104, 89779, 395014, \ldots.$$

Problem 213.6 – What is the number?

There is a certain positive integer. When divided by three it has remainder two; when divided by five it has remainder three; when divided by seven it has remainder two. What is the number?

Hint (translated from a 16th century Chinese song):

> *Three people walking together, 'tis rare that one be seventy,*
> *Five cherry blossom trees, twenty-one branches bearing flowers,*
> *Seven disciples reunite for the half-moon,*
> *Take away one hundred and fives and you shall know.*

—From *Introduction to Number Theory* by Hua Loo Keng.

Problem 213.7 – Orders

Tony Forbes

Let p be a prime. Let $\mathrm{ord}_p(x)$ denote the smallest positive integer y such that $x^y \equiv 1 \pmod{p}$. Thus y is the order of x modulo p.

Given p prime, characterize those pairs (x, y) for which both

$$\mathrm{ord}_p(x) \;=\; y \quad \text{and} \quad \mathrm{ord}_p(y) \;=\; x \qquad (*)$$

hold simultaneously.

If 2 is a primitive root modulo p, then (by definition) $\mathrm{ord}_p(2) = p - 1$. Also, since $(p-1)^2 \equiv 1 \pmod{p}$ and $p - 1 \neq 1$, we have $\mathrm{ord}_p(p-1) = 2$. So $(*)$ works for p, $x = 2$, $y = p - 1$ whenever 2 is a primitive root modulo p, as is the case for $p = 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, \ldots$. What about other triples (p, x, y) that satisfy $(*)$?

Problem 213.8 – Definite integral

Compute

$$\int_0^1 \frac{5x^{114} + 5x^{112} - \frac{4}{71}}{x^2 + 1}\, dx$$

to 8 decimal places.

Problem 213.9 – Balancing an ellipsoidal object

Tony Forbes

Suppose $a > 1$ and $k > 0$. An ellipsoid-like object of radii 1, 1 and a is defined by

$$(x^2 + y^2)^{k/2} + \left|\frac{z}{a}\right|^k \;\leq\; 1.$$

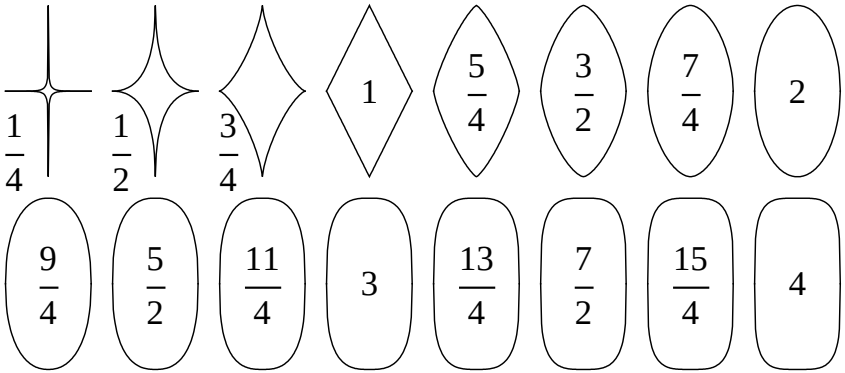
Alternatively, you can start with the curve

$$|x|^k + \left|\frac{z}{a}\right|^k \;=\; 1$$

in the (x, z)-plane and rotate it about the z-axis to get a solid of revolution.

For what values of a and k is it possible to balance the solid on one of its sharp ends?

[I am wondering if it is possible to do this with a rugby ball. If not and the game is played on a concrete pitch, it would surely be impossible to set it up for converting a try.]



Problem 213.10 – Minor axis

Another problem with an elliptical theme. A spherical globe with a clearly marked equator is thrown at random into the air and lands on the ground. The globe has diameter 1. Hence the projection of the equator on to the ground is an ellipse with major axis 1. What is the expected length of the minor axis?

Quasi-magic sudoku

ADF

The rules are as for standard sudoku—each row, column and 3×3 box must contain the symbols $\{1, 2, \ldots, 9\}$—but with an additional constraint. We also require that the rows, columns and diagonals of the nine 3×3 boxes must sum to 15 ± 3, i.e. any of 12, 13, 14, 15, 16, 17 or 18. So you can think of each box as a quasi-magic square of order 3.

							9	
9								
			9				1	
	2							6
		9		4		1		
5							8	
	1				8			
								8
	8							

Stocks of publishable material are running down. I think I have enough for M500 **214** but M500 **215** is beginning to look a little thin. In this issue I have given you more than the usual number of problems to work on—so do please get busy! But we also need articles, ideally 2–6 pages, especially stuff that can be understood by people who are just beginning university mathematics. Meanwhile, here is a small contribution from **Linda Forbes**.

Observe Doctor Frobes, who does nothing but probe
Into matters of prime import.
When not thinking of number
You'll find him in slumber,
Where he probably dreams of nought.

A fitting tribute. I look forward to the ceremony next June.—ADF

Contents M500 213 – December 2006