How to work with quotient rings?

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

Like any science, one investigates, conducts experiments and makes observations in order to see a pattern and make a guess in Mathematics. With an overwhelming emphasis on rigour, a typcial teacher does not want to explain how the result or a proof was arrived at. A case in point is the ability to guess what the quotient ring would be and how to work with it. It is the aim of this article to initiate the reader into the 'non-rigorous' way of thinking so that one gets to see a 'picture' and then proves rigorously what was observed.

Caution: We warn the pedantic readers or champions of rigour that they would find this article a real pain, as we exhbit our raw thought process with no heed for rigour at the preliminary stage of investigation.

Assume that we are quotienting a ring with respect to an ideal I. Let $\{a_i : i \in I\}$ be a set of generators of I. The basic intuition is that we are going to think of a_i (and hence 'ideal expressions' involving a_i) as the zero element (in the quotient ring). This will allow us to get an idea what the quotient ring may be. We then use the first fundamental theorem of homomorphism to prove our guess is correct (if it is!). Keep these vague ideas while going through the examples below. After going through them, we hope that students will be more comfortable while dealing with quotient rings.

Example 1. Let $I := \langle x - 5\rangle$ be the (principal) ideal generated by $x - 5$ in $R := \mathbb{Q}[x]$. We show that R/I is $\mathbb{Q}$.

The quotient must be a field since the polynomial $x - 5$ is irreducible so that the ideal $\langle x - 5\rangle$ is maximal.

Since $x - 5 = 0$ in the quotient ring, the basic intuition is that in any polynomial $p(x) \in \mathbb{Q}[x]$, we can replace x by 5. This means that if we have $ax^2 + bx + c$, then we read it as $a * 5^2 + b * 5 + c$. This suggests that the quotient must be $\mathbb{Q}$. Substituting 5 for x means that we are evaluating the polynomial at $x = 5$. We consider the evalution homomorphism $e_5 \colon \mathbb{Q}[x] \to \mathbb{Q}$ given by $p(x) \mapsto p(5)$. Clearly, $\langle x - 5\rangle \subset \ker e_5$. Let $p(x) \in \ker e_5$. We write $p(x) = (x - 5)q(x) + c$, by division algorithm. Then $p(5) = 0 + c = 0$ implies that $c = 0$, that is, $p \in \langle x - 5\rangle$. Hence we conclude that $\ker e_5 = \langle x - 5\rangle$. It is clear that the map is onto. By the first fundamental theorem of homomorphism, we conclude that the quotient ring is isomorphic to $\mathbb{Q}$.

Example 2. $\mathbb{Z}_n$ as a quotient of $\mathbb{Z}$.

Consider the map $f\colon \mathbb{Z} \to \mathbb{Z}_n$ given by $k \mapsto [k]$ where $[k]$ stands for the congruence class of k modulo n. Thus, $[k] = [r]$ if we write $k = qn + r$ using division algorithm. It is well-known that f is a ring homomorphism and the kernel is $I = n\mathbb{Z}$, the ideal of all multiples of n. Hence by the first fundamental theorem of homomorphism, we conclude that $\mathbb{Z}/\langle n\rangle$ is isomorphic to $\mathbb{Z}_n$.

Example 3. $\mathbb{R}[x]/\left\langle 1 + x^2\right\rangle$ as $\mathbb{C}$.

Here again, the intuition is that whenever we see x^2, we can replace it by -1. Thus, if x^3 is read as $x^2 * x = -x$, then $2 + x^2 = 2 - 1 = 1$ etc. If $n = 2k + 1$, then x^n is interpreted as $(x^{2k}) * x = (-1)^k x$. Thus any polynomial $p(x)$ will "reduce" to one of the form $a + bx$.

Also, if we multiply $(ax+b)(cx+d) = acx^2+(ad+bc)x+bd$, it is read as $(bd-ac)+(ad+bc)x$. This suggests that the multiplication looks like the multiplication of complex numbers and (the coset of) x behaves like $i = \sqrt{-1}$. So, the quotient ring may be the field of complex numbers. We now prove this rigorously.

Consider the map $f\colon \mathbb{R}[x] \to \mathbb{C}$ given by $p(x) \mapsto p(i)$. Clearly, $\left\langle x^2 + 1\right\rangle \subset \ker f$. To prove the converse, let $p(x) \in \ker f$. Using division algorithm, we write $p(x) = (x^2 + 1)q(x) + (a + bx)$. Then $0 = f(p) = f((x^2 + 1)q(x)) + a + bi = a + bi$. Hence $a = 0 = b$, in other words, $p \in \left\langle x^2 + 1\right\rangle$, The map is obviously onto. Hence by the first fundamental theorem of homomorphism, the claim follows.

Ex. 4. Show that $\mathbb{Z}[x]/\left\langle x^2 + 1\right\rangle$ is the ring of Gaussian integers.

Example 5. Consider $\frac{\mathbb{Q}[x]}{\langle x^2+2x+2\rangle}$. Since $x^2 + 2x + 2$ is irreducible in $\mathbb{Q}[x]$, the quotient ring is a field. We show that the inverse of the coset $[x^3 + 1]$ is $-[\frac{4}{13}\left(\frac{x}{2} - \frac{1}{4}\right)]$.

The trick is to use the Euclidean algorithm.

$$\begin{aligned} x^3 + 1 &= (x - 2)(x^2 + 2x + 2) + (2x + 5) \\ x^2 + 2x + 2 &= \left(\frac{x}{2} - \frac{1}{4}\right)(2x + 5) + \frac{13}{4}. \end{aligned}$$

Hence we get

$$\begin{aligned} \frac{13}{4} &= (x^2 + 2x + 2) - \left(\frac{x}{2} - \frac{1}{4}\right)(2x + 5) \\ &= (x^2 + 2x + 2) - \left(\frac{x}{2} - \frac{1}{4}\right)\left((x^3 + 1) - (x - 2)(x^2 + 2x + 2)\right) \\ &= p(x)(x^2 + 2x + 2) - \left(\frac{x}{2} - \frac{1}{4}\right)(x^3 + 1), \end{aligned}$$

where $p(x)$ is some polynomial. Hence we get

$$1 = -\frac{4}{13}\left(\frac{x}{2} - \frac{1}{4}\right)(x^3 + 1) \text{ modulo } x^2 + 2x + 2.$$

Ex. 6. In the quotient ring $\frac{\mathbb{Z}_3[x]}{\langle x^3+2x+1\rangle}$, show that

(i) $[x^2 + x + 2][2x^2 + 1] = [x^2]$.
(ii) $[x^2 + 1]^{-1} = [2x^2 + x + 2]$.

Example 7. We show that $\langle x - y^2 \rangle$ is a prime ideal in $\mathbb{R}[x, y]$ by showing that that quotient ring is an integral domain. The idea here is that in the polynomial ring $\mathbb{R}[x, y]$, we replace x by y^2. It is 'obvious' that we get only polynomials in y. Thus, we expect the quotient ring to be a polynomial ring in one variable. We now prove this.

Consider the ring homomorphism $\varphi\colon \mathbb{R}[x, y] \to \mathbb{R}[t]$ given by $\varphi(x) = t^2$ and $\varphi(y) = t$. (To make sure you understand, find out the images of some concrete examples of polynomials and then later of a polynomial of the form $\sum_{i,j} a_{i,j} x^i y^j$. Check that φ is a surjective ring homomorphism.) Clearly, $\langle x - y^2 \rangle \subset \ker \varphi$. Let $p(x, y) \in \ker \varphi$.

Let $S := R/I$ where $I := \langle x - y^2 \rangle$. A polynomial $f(x, y)$ in the variables x, y can be written as a polynomial in y with coefficients in $\mathbb{R}[x]$. Since $y^2 = x$ modulo $(x - y^2)$, $f(x, y)$ is a linear polynomial in y with coefficients in $\mathbb{R}[x]$ modulo $(x - y^2)$. This motivates the claim: every element of S can be written in the form $p(x) + q(x)y + I$, for $p, q \in \mathbb{R}[x]$. To prove this, consider an arbitrary coset $f(x, y) + I \in S$. Then we can write this as

$$\begin{aligned} f(x,y) + I &= q(x) + \text{ terms with odd powers of } y + \text{ terms with even powers of } y + I \\ &= q(x) + y \cdot \text{ terms with even powers of } y + \text{ terms with even powers of } y + I. \end{aligned}$$

Since any term with an even power of y is of the form $g(x)y^{2k}$ and since $x + I = y^2 + I$, we see that we can replace the second and third terms above by terms of the form $h_1(x)y + I$ and $h_2(x) + I$. Hence the claim follows.

We are now ready for the kill. Let $f(x, y) \in \ker \varphi$. Using the claim, we write $f(x, y) = g(x) + h(x)y + \psi(x, y)$ where $\psi \in I$. Now, we operate φ on both sides of the equation to get

$$\varphi(f)(t) = g(t^2) + h(t^2) \cdot t = 0.$$

Noting that there are no common powers of t in the two terms $g(t^2)$ and $h(t^2) \cdot t$, we see that the coefficients of g and h must be zero. Hence $f = \psi \in I$.

Example 8. We let $\mathcal{C}$ be the ring of Cauchy sequences of rational numbers and $\mathcal{N}$ the set of sequences of rational numbers converging to 0. We show that $\mathcal{N}$ is a maximal ideal of $\mathcal{C}$. We also identify the quotient ring. It should not be a surprise that we need real analysis for this problem.

Let $(x_n) \in \mathcal{C}$. Since (x_n) is a Cauchy sequence of rational numbers and hence *a priori* a Cauchy sequence of real numbers, it is convergent to a real number, say x. If (x_n) and (y_n) in $\mathcal{C}$ are such that their difference $(x_n - y_n) \in \mathcal{N}$, we know that both converge to the same real number. These considerations suggest that the quotient ring is $\mathbb{R}$.

The proof is an exercise in real analysis. Consider the map $f\colon \mathcal{C} \to \mathbb{R}$ given by $f((x_n)) := \lim x_n$, where $\lim x_n$ is the real number to which (x_n) converges. By the algebra of limits, the map f is a ring homomorphism. By the very definition, the kernel of f is $\mathcal{N}$. Also, by the density of $\mathbb{Q}$ in $\mathbb{R}$, we know that for any given $x \in \mathbb{R}$, and for any $n \in \mathbb{N}$, there exists a rational $x_n \in (x - \frac{1}{n}, x + \frac{1}{n})$. Clearly, $(x_n) \in \mathcal{C}$ and we have $f((x_n)) = x$. Hence f is onto. Now the first fundamental theorem of homomorphism tells us the quotient ring $\mathcal{C}/\mathcal{N}$ is $\mathbb{R}$ and hence $\mathcal{N}$ is a maximal ideal in $\mathcal{C}$.

Example 9. Let $I := \langle x^2 - y^3 \rangle$ and $R := \mathbb{R}[x, y]$. We identify the quotient ring R/I as the subring of $\mathbb{R}[t]$ consisting of polynomials in t in which the coefficient of t is zero.

This time, we are looking for a ring A and an onto ring homomorphism $f\colon R \to A$ whose kernel is $\langle x^2 - y^3 \rangle$. Based on our experience with earlier examples, we may think of $A = \mathbb{R}[t]$ and $f(x) = t^3$, and $f(y) = t^2$.

Consider the map $f\colon R \to A$ given by $f(p(x,y)) = p(t^3, t^2)$. It is easy to verify that f is a ring homomorphism. Try out this map with some specific polynomials in x and y to gain some idea of what is happening. You may find that the first degree term is absent in the image polynomials in t. Since we want an onto map, we take the subring S of polynomials in t with the property that the coefficient of the first degree term is zero as the codomain of the map f. It is easy to see that $f\colon R \to S$ is onto. $p(x,y) := a_0 + a_2 y + a_3 x + a_4 y^2 + \ldots$ is its pre-image. For example, $t^5 = f(xy)$, $t^9 = f(x^2 y)$ etc.

We now show that $\ker f = \langle x^2 - y^3 \rangle$. We need only show that if $p(x,y) \in \ker f$, then $p(x,y) + \langle x^2 - y^3 \rangle = \langle x^2 - y^3 \rangle$. We claim that

$$p(x,y) = p_1(y) + p_2(y)x \text{ modulo } (x^2 - y^2). \tag{1}$$

To prove this we observe

$$p(x,y) = p_1(y) + \text{ terms with even powers of } x + \text{ odd powers of } x.$$

Let us look at a typical 'even power' term $x^{2k} y^r = y^{3k} y^r = y^{3k+r}$ modulo $(x^2 - y^3)$. On the other hand, we have $x^{2k+1} y^r = x y^{3k+r}$ modulo $(x^2 - y^3)$. Hence the claim (1) follows. If we now apply φ to both side of (1), we get

$$0 = p_1(t^2) + p_2(t^2) t^3.$$

The first term on the right side has only even powers of t while the second has only odd powers of t. Hence we conclude that $p_1 = 0 = p_2$. That is, $p(x,y) = 0$ modulo $(x^2 - y^3)$.

Example 10. We claim that $\mathbb{R}[x,y]/(x-y)$ is $\mathbb{R}[t]$. This is intuitively clear since in a polynomial $p(x,y)$ we can replace y by x so that we get finally a polynomial in a single variable x.

We prove this rigorously as follows: Consider $\varphi\colon \mathbb{R}[x,y] \to \mathbb{R}[t]$ by setting $\varphi(p(x,y)) = p(t,t)$. Clearly, $(x-y) \subset \ker \varphi$. We show the reverse inclusion as in the last Example 9. Let $\varphi(p(x,y)) = 0$.

$$\begin{aligned} p(x,y) &= a, \text{ the constant term } + \text{terms with either the power of } x \text{ or of } y \text{ being positive} \\ &= a + p_1(x) \text{ modulo the ideal } < x - y > \text{ with constant term of } p_1 \text{ equal to } 0. \end{aligned}$$

Hence $\varphi(p(x,y)) = 0$ implies that $a + p_1(t) = 0$, that is $a = 0$ and $p_1 = 0$. Thus, $p(x,y) = 0$ modulo the ideal $< x - y >$. By now, the reader should know how to complete the story.

Example 11. We compute the quotient ring $\mathbb{Z}[i]/(1+2i)$. The ring $\mathbb{Z}[i]$ is generated by $1, i$. Now the ideal gives a relation between them, namely, $2i = -1$ and hence $-4 = 1$. Thus, in the quotient, we should expect $5 = 0$, that is, the quotient ring must have 5 as its characteristic. Since 1 of the ring will go 1 of the quotient ring, we need to see where i goes to. Now, $1 + 2i = 0$ implies "$i = -(1/2)$", that is, "i is the additive inverse of the multiplicative inverse of 2" in the quotient ring. In $\mathbb{Z}_5$, we have the multiplicative inverse of 2 as 3 whose additive inverse is 2. This suggests that we consider the map

$$\varphi\colon \mathbb{Z}[i] \to \mathbb{Z}_5 \text{ given by } \varphi(1) = [1] \text{ and } \varphi(i) = [2], \varphi(a + ib) = [a + 2b].$$

It is easy see that φ is an onto ring homomorphism such that $(1+2i) \subset \ker\varphi$. Let $a+ib \in \ker\varphi$. This means that $a+2b = 5k$ for some $k \in \mathbb{Z}$, or $a = 5k-2b$. We have

$$\begin{aligned} a+ib &= (5k-2b)+ib \\ &= 5k+ib(1+2i) \\ &= (1+2i)(1-2i)k+ib(1+2i) \\ &= (1+i(b-2k))\,(1+2i) \\ &\in (1+2i). \end{aligned}$$

Thus $\ker\varphi = (1+2i)$. We have thus proved that the quotient ring is $\mathbb{Z}_5$.

Example 12. We show that the quotient ring $\mathbb{R}[x,y]/\langle xy\rangle$ is isomorphic to

$$\{(p,q) : p(t), q(t) \in \mathbb{R}[t] \text{ with } p(0) = q(0)\}.$$

(You may check that the above subset is a subring of the ring $\mathbb{R}[t]\times\mathbb{R}[t] = \mathbb{R}[t]\oplus\mathbb{R}[t]$.) Since x and y commute and $[x][y] = 0$, the quotient ring is a commutative ring (with multiplicative identity and) with zero divisors. Also, [1], $[x]$ and $[y]$ generate the quotient. Further, there is no other relation between $[x]$ and $[y]$ implying that no polynomial expression in $[x]$ and $[y]$ without mixd terms can collapse in the quotient ring. This suggests that the quotient ring may be something like a direct sum of two polynomial rings, say, $\mathbb{R}[u]\oplus\mathbb{R}[v]$. (In fact, in the first attempt, we claimed this!) So, we consider the ring homomorphism $\varphi\colon \mathbb{R}[x,y] \to \mathbb{R}[u]\oplus\mathbb{R}[v]$ defined by setting $\varphi(1) = (1,1)$, $\varphi(x) = (u,0)$ and $\varphi(y) = (0,v)$. Let us determine the image of φ. If $p(x,y) = a_0 + \sum_{i+j=k} a_{ij}x^iy^j$, then

$$\varphi(p(x,y)) = a_0(1,1) + \sum_{i+j=k} a_{ij}(u^i,0)(0,v^j) = (a_0+p_1(u), a_0+p_2(v)), \text{ say.}$$

Thus the image lies in $\{(f(u),g(v)) : f(0) = g(0)\}$. We leave it to the reader to check that this is the image of φ.

Clearly, $\langle xy\rangle \subset \ker\varphi$. Let $p(x,y) \in \ker\varphi$. We have

$$p(x,y) \;=\; \left(\sum_r a_r x^r + \sum_s b_s y^s\right) \text{ modulo } (xy).$$

Hence, we see that

$$0 = \varphi(p(x,y)) = \sum_r a_r(u,0)^r + \sum_s b_s(0,v)^s$$

implies that $a_r = 0 = b_s$ for all r and s. Thus, $p(x,y) = 0$ modulo the ideal (xy). Hence the quotient ring is as specified.

Example 13. We show that the quotient $\mathbb{R}[x,y]/(xy-1)$ is the 'localization' of $\mathbb{R}[t]$ with respect to the multiplicative set $\{t^n : n \in \mathbb{Z}_+\}$.

The idea here is that we can replace y by $1/x$. Thus, $x^my^n \mapsto x^{m-n}$ where $x^r = (1/x^{-r})$ if $r < 0$. Hence we expect the quotient ring would be the ring $\mathbb{R}[t]_{(t)}$ of Laurent polynomials in a variable t, that is, polynomials in t and $1/t$. (Another way of looking at the ring of Laurent polynomials is that it is got by localising the polynomial ring $\mathbb{R}[t]$ with respect to

the multiplicative set $\{t^n : n \in \mathbb{N}\}$. If you have not seen the concept of localisation earlier, you may skip this explanation.)

Consider the map $\varphi\colon \mathbb{R}[x,y] \to \mathbb{R}[t]_{(t)}$ given by $\varphi(p(x,y)) = p(t,1/t)$. It is easy to check that this is a ring homomorphism and that $(xy-1) \subset \ker\varphi$. Let $p(x,y) \in \ker\varphi$. Let us look at a typical term x^iy^j:

$$\begin{aligned} x^iy^j &= (xy)^iy^{j-i} = y^{j-i} \text{ modulo } (xy-1) \text{ if } i \le j \\ &= (xy)^jx^{i-j} = x^{i-j} \text{ modulo } (xy-1) \text{ if } j \le i. \end{aligned}$$

Hence we see that $p(x,y) = (p_1(x) + p_2(y))$ modulo $(xy-1)$. Thus, if $\varphi(p(x,y)) = 0$, then we get $\varphi(p_1(x)) + \varphi(p_2(y)) = p_1(t) + p_2(1/t) = 0$. This means that $p_1(x) = 0$ and $p_2(y) = 0$. In other words, if $p(x,y) \in \ker\varphi$, then $p(x,y) = 0$ modulo $(xy-1)$.

Another important tool is the third isomorphism theorem:

If $I \subseteq J$ are ideals of R then $R/J \simeq (R/I)/(J/I)$.

This is useful in the following way. If the ideal J is generated by two elements, say, $J =< a,b >$, then $R/J = R/ < a > /(< a,b > / < a >)$. A useful remark is that it is up to us to choose which is the first element we want to 'equate' to 0! The following example will illustrate this.

Example 14. What is the quotient ring $\mathbb{Z}[i]/ < 2 >$? We may think of this ring as the quotient ring $\mathbb{Z}[x]/ < x^2+1, 2 >$. We then quotient $\mathbb{Z}[x]$ first by $< 2 >$ to get $\mathbb{Z}_2[x]$ in which we have to use '$x^2 = 1$' or '$x = i$'. We find that the elements of $\mathbb{Z}_2[x]/ < 1 + x^2 >$ can be written in the form $a + bx$ with $a, b \in \mathbb{Z}_2$ with the relation $x^2 = -1$. Thus the elements can be written as $0, 1, i, 1+i$ (or 0, 1, x and $1+x$). The element $(1+i)^2 = 0$ and is therefore a nilpotent. Similarly, $i(1+i) = i - 1 = i + 1$ etc. Though as a group the quoteint $\mathbb{Z}[i]/ < 2 >$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, they are not isomorphic as rings. (Why?)

Example 15. Consider the quotient ring $\mathbb{Z}[x]/ < x^3 + x + 1, 5 >$. We want to show that the ideal $< x^3 + x + 1, 5 >$ is maximal in $\mathbb{Z}[x]$. We wish to prove this by showing the quotient $\mathbb{Z}[x]/ < x^3 + x + 1, 5 >$ is a field. We may first quotient $\mathbb{Z}[x]$ by $< 5 >$ to get $\mathbb{Z}_5[x]$. Now it is eaily seen that $x^3 + x + 1$ is irreducible in $Z_5[x]$ by a straight-forward computation, namely by showing that no element of $\mathbb{Z}_5$ is a zero of the polynomial. Hence the claim follows.

Example 16. What are the quotient rings of $\mathbb{Z}_{12}$? To answer this, we need to find the ideals in $\mathbb{Z}_{12}$. This is well-known because of the correspondence between the ideals $\overline{J}$ in the quotient ring R/I and the ideals J (in R) containing I. Thus, the ideals in $\mathbb{Z}_{12}$ "correspond" to the ideals $< d >$ where d is a divisor of 12. Now the ideals in $\mathbb{Z}$ that contain $< 12 >$ are $< 1 >, < 2 >, < 3 >, < 4 >, < 6 >, < 12 >$. Hence the ideals in $\mathbb{Z}_{12}$ are $\mathbb{Z}_{12}$, $\{0,2,4,6,8,10\}$, $\{0,3,6,9\}$, $\{0,4,8\}$ $\{0,6\}$ and $\{0\}$. As groups the corresponding quotient groups are $\mathbb{Z}_d$, where $d = 1, 2, 3, 4, 6, 12$. These group homomorphisms preserve the multiplication and hence they are ring isomorphisms. (Note that, by the third isomorphism theorem, $\mathbb{Z}_{mn}/\langle n \rangle \simeq \mathbb{Z}_n$.) Hence we have found all the quotient rings of $\mathbb{Z}_{12}$.

Example 17. When is $\mathbb{Z}_3[x]/ < x^3 + x + c >$ a field? It is well-known that the quotient is a field iff the polynomial $p(x) := x^3 + x + c$ is irreducible. Again, being cubic, $p(x)$ is irreducible iff it does not have a root in $\mathbb{Z}_3$. Now, if $c = 0$, then $x = 0$ is a root and hence $p(x)$ is not irreducible. If $c = 1$, then $x = 1$ is a root. It is easily verified that if $c = 2$, the polynomial $p(x)$ has no roots in $\mathbb{Z}_3$. Hence the quotient ring is a field iff $c = 2$.

Example 18. Consider the ring $\mathbb{Z}_5[x]/ < x^2+1 >$. The ring has 25 elements as any element is of the form $a + bx$, with $a, b \in \mathbb{Z}_5$. (Why?) However, the ring is not a field, since we have

$$(x+2)(x+3) = 0 \text{ modulo the ideal } < x^2+1 > .$$

Thus the ring has zero divisors.

Example 19. One can similarly prove the following:

(i) $\mathbb{Z}[x]/ < x^2 - x - 1, 2 >$ is a field of 4 elements, say, [0], [1] $[x]$, and $[1 + x]$. The multilicative inverses of the nonzero elements (in the order of listing) are [1], $[1 + x]$ and $[x]$. *Hint:* In $Z_2[x]$ use "$x^2 = 1 + x$".

(ii) $\mathbb{Z}[x]/ < x^3 - x - 1, 2 >$ is a field of 8 elements.

(iii) $\mathbb{Z}[x]/ < x^2 + 1, 3 >$ is a field of 9 elements.

Remark 20. A set of notes written by Ashish Bansal based on my lectures in MTTS 2007 (Level 2) was useful in some of the examples in this article. I thank the referee for poining out a sign problem in Example 5 and suggestions that improved the readability of this article.