Real polynomials on the unit circle

Rahbar Virk
Department of Mathematics
University of Wisconsin
Madison, WI 53706
virk@math.wisc.edu

March 1, 2007

Proposition. *Let* $R = \mathbb{R}[x,y]/ < x^2 + y^2 - 1 >$.

1. *R is a Dedekind domain.*

2. *If $\mathfrak{p}$ is a prime (and thus maximal) ideal in R, then $R/\mathfrak{p}$ is an algebraic extension of $\mathbb{R}$, and thus isomorphic to either $\mathbb{R}$ or $\mathbb{C}$. Both possibilities can occur, in the first case $\mathfrak{p}$ is of the form $\langle x-\alpha, y-\beta\rangle$, where $\alpha,\beta \in \mathbb{R}$ and $\alpha^2+\beta^2 = 1$, and in the second case, $\mathfrak{p}$ is a principal ideal generated by some linear polynomial $y+b$, where $b \in \mathbb{R}$, $|b| > 1$, or $x+ay+b$, where $a,b \in \mathbb{R}, b^2 - a^2 > 1$. The class group is generated by the classes of the ideals $\langle x-\alpha, y-\beta\rangle$, where $\alpha,\beta \in \mathbb{R}$ and $\alpha^2+\beta^2 = 1$.*

3. *If $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals of the form $\langle x-\alpha_j, y-\beta_j\rangle$, respectively, where $\alpha_j^2+\beta_j^2 = 1, j = 1,2$, then $\mathfrak{p}_1\mathfrak{p}_2$ is aprincipal ideal, with generator a linear polynomial vanishing at both (α_1,β_1) and $)\alpha_2,\beta_2)$, if these points are distinct or else the linear polynomial $\alpha_1 x+\beta_1 y-1$ if $\mathfrak{p}_1 = \mathfrak{p}_2$. Thus, all non-principal prime ideals of R define the same element of the class group, this element is of order 2 and hence the class group is isomorphic to $\mathbb{Z}/2$.*

Proof. To show that R is a Dedekind domain it suffices to show that R is a commutative integral domain such that every non-zero prime ideal is maximal, it is integrally closed in its field of fractions and it is noetherian.

Note that x^2+y^2-1 is irreducible in $\mathbb{R}[x,y]$ (a UFD) and hence prime making R an integral domain.

Also note that $\mathbb{R}[x,y]$ may be viewed as the ring of polynomials in one indeterminate (y) over the ring $\mathbb{R}[x]$. R is simply an algebraic extension of $\mathbb{R}[x]$, i.e, $R \cong \mathbb{R}[x](\sqrt{1-x^2})$ (the isomorphism is given by the obvious map).

Now let $\mathfrak{p}$ be a non-zero prime ideal in R and let $f_1(x) + f_2(x)\sqrt{1-x^2} \in \mathfrak{p}$. Now $(f_1(x) - f_2(x)\sqrt{1-x^2})(f_1(x) + f_2(x)\sqrt{1-x^2}) = f_1^2(x) - f_2^2(x)(1-x^2) \in \mathbf{p}$ and thus $\mathfrak{q} = \mathfrak{p} \cap \mathbb{R}[x]$ is a non-zero prime ideal in $\mathbb{R}[x]$ and is hence maximal (as $\mathbb{R}[x]$ is a PID).

We thus have that $\mathbb{R}[x]/\mathbf{q}$ is a field. Now note that $R/\mathfrak{p}$ is a finite dimensional vector space over $\mathbb{R}[x]/\mathfrak{q}$ (R as a module is finitely generated over $\mathbb{R}[x]$ and $\mathbb{R}[x]/\mathfrak{q}$ is isomorphic to the image of $\mathbb{R}[x]$ in $R/\mathfrak{p}$). We need to show that $R/\mathfrak{p}$ is a field. Let $z \neq 0$ be in $R/\mathfrak{p}$. As we are in a finite dimensional vector space there must be a nontrivial expression of the form

$$a_0 + a_1 z + a_2 z^2 + \cdots + a_k z^k = 0$$

with $a_0, \ldots, a_k \in \mathbb{R}[x]/\mathfrak{q}$ and not all a_i zero. Let k be minimal then $a_0 \neq 0$ as otherwise we could cancel a factor z (as $\mathfrak{p}$ is prime, $R/\mathfrak{p}$ is a domain and we have cancellation in products). Thus

$$(a_1 z + \cdots + a_k z^k) = a_0$$

now $a_0 \in \mathbb{R}[x]/\mathfrak{q}$ which is a field so

$$a_0^{-1} z(a_1 + \cdots + a_k z^{k-1}) = 1$$

and z is a unit.

To see that R is integrally closed, first note that $\mathbb{R}[x]$ by virtue of being a UFD is integrally closed. Now let F be the field of fractions for $\mathbb{R}[x]$. Now let $\alpha = \sqrt{1-x^2}$ and note that $R = \mathbb{R}[x](\alpha)$ and the field of fractions of R is $F(\alpha) = F + F\alpha$ i.e every element of $\zeta \in F(\alpha)$ can be written as $\zeta = m + n\alpha$ with $m, n \in F$. Now if ζ is integral over R then by 'transitivity of integrality' then ζ is integral over $\mathbb{R}[x]$. The minimal polynomial of ζ over F is $X^2 - 2mX + (m^2 - n^2(1-x^2))$. As the ζ is integral over $\mathbb{R}[x]$ and the minimal polynomial is unique we have $2m \in \mathbb{R}[x]$ and hence $m \in \mathbb{R}[x]$, furthermore $m^2 - n^2(1-x^2) \in \mathbb{R}[x]$ which gives us that $n^2(1-x^2) \in \mathbb{R}[x]$. Now as $\mathbb{R}[x]$ is a UFD if some prime p of $\mathbb{R}[x]$ divides the denominator of n then $p^2 | 1 - x^2$ but $1 - x^2$ is square free and hence $n \in \mathbb{R}[x]$ which gives us that $\zeta \in F(\alpha) = R$.

Furthermore, it is quite clear that R is noetherian, hence we have shown that R is a Dedekind domain.

We will now characterize all prime (and hence maximal) ideals of R. First of all note that if $f \in R$ then f can be represented as $p_1(x) + p_2(x)y$ and as $g_1(y) + g_2(y)x$ where p_1, p_2, g_1, g_2 are polynomials over the reals. Now let $\mathfrak{p}$ be a proper prime ideal of R and assume that it has two minimal generators, i.e $\mathfrak{p} = \langle f(x,y), g(x,y) \rangle$. From our earlier observation $f(x,y) = f_1(x) + f_2(x)y$ and note that $(f_1(x) - f_2(x)y)f(x,y)$ can be represented as an element of $\mathbb{R}[x]$ and as this element is in $\mathfrak{p}$ we can obtain an irreducible (over $\mathbb{R}[x]$) polynomial in the ideal. As this polynomial is irreducible over the reals we have

Case 1 The irreducible polynomial obtained is of the form $x - \alpha$. Now $g(x,y) = g_1(x) + g_2(x)y$ and we can divide g_1 and g_2 by $x - \alpha$ to get a polynomial $h(x,y) = y - \beta$ such that $\langle x - \alpha, y - \beta \rangle = \mathfrak{p}$. Also note that using the relation $x^2 + y^2 = 1$ we get that $\alpha^2 + \beta^2 = 1$ as otherwise $\mathfrak{p}$ would be the whole ring.

Case 2 The irreducible polynomial obtained is of the form $x^2 + ax + b$, we can obtain another irreducible polynomial using the other representation of f in terms of y, if this polynomial is linear then we are back in the situation of case, otherwise we have a quadratic in y which can be added with the quadratic in x to obtain a polynomial of the form $x + ay + b$ (or $y + sx + t$, without loss of generality we may assume that it is of the former form), modding out this polynomial from g to obtain another distinct polynomial of the form $x + a_1 y + b_1$ (it must be distinct as our ideal is 2-generated). Using these two polynomials we obtain $y - \beta \in \mathfrak{p}$ and we are back in the situation of case 1.

Now assume $\mathfrak{p}$ is principal, then using the same arguments as before we can obtain an irreducible polynomial over the reals, if this is linear then we have a generator of the form $y - \beta$ (or symmetrically $x - \alpha$), without loss of generality we may assume it is the former (as we will cover the other form when we deal with the quadratic case next), now clearly $|\beta| > 1$ as otherwise as case 1 of the 2-generated case has shown we wont have a maximal ideal.

Now if our irreducible was a quadratic then using the arguments of case 2 from the 2-generated case we obtain a polynomial of the form $x + ay + b$. Now $b^2 - a^2 > 1$ as otherwise using the relation $x^2 + y^2 = 1$ we get that

$$x + ay + b = (a^2 + 1)y^2 + 2aby + b^2 - 1 = (a^2 + 1)(y - \zeta)(y - \overline{\zeta})$$

where $\zeta = \frac{-2ab+2\sqrt{a^2-b^2+1}}{2(a^2+1)}$ and $\overline{\zeta}$ is it's galois conjugate, which contradicts the fact that we had an irreducible.

Also, the statement about $R/\mathfrak{p}$ as an algebraic extension of $\mathbb{R}$ follows easily from our characterizations of $\mathfrak{p}$.

Finally, let $\mathfrak{p}_1 = \langle x - \alpha_1, y - \beta_1 \rangle$ and $\mathfrak{p}_2 = \langle x - \alpha_2, y - \beta_2 \rangle$, thus $\mathfrak{p}_1\mathfrak{p}_2 = \langle f, g, h, p \rangle$ where

$$\begin{aligned} f &= x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2 \\ g &= xy - \beta_2 x - \alpha_1 y + \alpha_1\beta_2 \\ h &= xy - \beta_1 x - \alpha_2 y + \alpha_2\beta_1 \\ p &= y^2 - (\beta_1 + \beta_2)y + \beta_1\beta_2 \end{aligned}$$

Observe that every element of $\mathfrak{p}_1\mathfrak{p}_2$ vanishes at (α_1, β_1) and (α_2, β_2). If $\mathfrak{p}_1 \neq \mathfrak{p}_2$ it follows that if we have any two linear polynomials (i.e of the form $ax + by + c$) in $\mathfrak{p}_1\mathfrak{p}_2$ then they must be scalar multiples of each other (as otherwise we could "solve" the system of equations and obtain a polynomial which does not vanish at both points). Note that $f + p$ and $g - h$ are linear, thus if we can show that $\langle f + p \rangle$ contains f and g then $\langle f + p \rangle = \mathfrak{p}_1\mathfrak{p}_2$. Now if $\alpha_1 + \alpha_2 \neq 0$ then $(f + p)(-ax - by - c) = f$ and $(f + p)(rx + sy + t) = g$, where

$$\begin{aligned} a &= \frac{\alpha_1 + \alpha_2}{2(1 + \alpha_1\alpha_2 + \beta_1\beta_2)} \\ b &= \frac{\beta_1 + \beta_2}{-2(1 + \alpha_1\alpha_2 + \beta_1\beta_2)} \\ c &= \frac{-1}{2} \\ r &= \frac{\beta_1 + \beta_2}{2(1 + \alpha_1\alpha_2 + \beta_1\beta_2)} \\ s &= \frac{\beta_1 - \beta_2}{2(\alpha_1 + \alpha_2)} \\ t &= \frac{1 + \alpha_1^2 - \beta_2^2 + 2\alpha_1\alpha_2}{2(\alpha_1 + \alpha_2)(1 + \alpha_1\alpha_2 + \beta_1\beta_2)} \end{aligned}$$

(Note that the condition $\alpha_1 + \alpha_2 \neq 0$ is enought as $1 + \alpha_1\alpha_2 + \beta_1\beta_2 = (\alpha_1 + \alpha_2)^2 + (\beta_1 + \beta_2)^2$) If $\mathfrak{p}_1 = \mathfrak{p}_2$ then the same argument still works as $g - h = 0$. Thus, the only case we are left with is when $\alpha_1 + \alpha_2 = 0$ and hence $\beta_1 = \pm\beta_2$.

Case 1 $\beta_1 = \beta_2$, then

$$\begin{aligned} f &= x^2 - \alpha_1^2 \\ g &= xy - \beta_1 x - \alpha_1 y + \alpha_1\beta_1 \\ h &= xy - \beta_1 x + \alpha_1 y - \alpha_1\beta_1 \\ p &= y^2 - 2\beta_1 y + \beta_1^2 \\ f + p &= -2\beta_1(y - \beta_1) \end{aligned}$$

$g - h$ is still linear, and clearly if $\beta_1 \neq 0$ then $y - \beta_1 \in \mathfrak{p}_1\mathfrak{p}_2$, moreover $(y - \beta_1)(-y - \beta_1) = f$ and clearly $p \in \langle y - \beta_1 \rangle$, thus $\mathfrak{p}_1\mathfrak{p}_2 = \langle y - \beta_1 \rangle$. If $\beta_1 = 0$ then $\alpha_1^2 = 1$ and it follows easily that $\mathfrak{p}_1\mathfrak{p}_2 = \langle y \rangle$.

Case 2 $\beta_1 = -\beta_2$, then

$$\begin{aligned} f &= x^2 - \alpha_1^2 \\ g &= xy + \beta_1 x - \alpha_1 y - \alpha_1\beta_1 \\ h &= xy - \beta_1 x + \alpha_1 y - \alpha_1\beta_1 \\ p &= -f \\ f + p &= 0 \\ g - h &= 2(\beta_1 x - \alpha_1 y) \end{aligned}$$

$\frac{-1}{2}(\alpha_1 x - \beta_1 y)(g - h) = xy - \alpha_1\beta_1$, thus $g, h \in \langle g - h \rangle$, furthemore $\frac{1}{2}(\beta_1 x + \alpha_1 y)(g - h) = f$ and hence $\mathfrak{p}_1\mathfrak{p}_2 = \langle g - h \rangle$.

It now follows clearly that the class group of R is $\mathbb{Z}/2$.

□