ON THE FROBENUIS THEOREM ON REAL DIVISION ALGEBRAS

MICHAEL BARR

1. Introduction.

The Frobenius theorem states that a finite dimensional division algebra over the reals is one of the reals $\mathbf{R}$, the complex numbers $\mathbf{C}$ or the quaternions $\mathbf{H}$. Recently, Peter Freyd showed me a proof that is simpler than the known proofs. Assuming the dimension is not 1, it uses conjugation by a square root of -1 to simplify the argument. We outline his proof. It is valid on the assumption that R is a real closed field and A is a finite dimensional R-algebra with no zero divisors. In addition, we give an example that shows that the result fails if we don't suppose that $\mathbf{R}$ lies in the center of the algebra.

2. Peter Freyd's proof.

If K is a commutative ring, then by a K-algebra A we mean a ring together with a additive map $K \otimes A \to A$ that satisfies the equations $k(aa') = (ka)a' = a(ka')$ for $k \in K$ and $a, a' \in A$. We do not assume that either ring contain an identity. But if they do these equations imply that the induced image of $K \to A$ lies in the center of A.

An ordered field is called real closed if no algebraic extension can be ordered. Real closed fields are characterized by the facts that every positive element has a square root in and every odd order polynomial has a root. In an ordered field, -1 cannot have a square root, but if R is real closed then $C = R[i]$ is algebraically closed, where i is a square root of -1.

The proof of the last is the same as that of one of the standard proofs that the complex numbers is algebraically closed. Take an irreducible polynomial and adjoin all its roots. Let G be the Galois group and H be a 2-Sylow subgroups of G. Then $\mathrm{Fix}(H)$ is an odd order extension of R, which is not possible since every odd order polynomial has a root in R. Thus G is a 2-group. Since p-groups are solvable, the extension is by a sequence of square roots. The first step in the sequence must be to adjoin the square root of a negative number since positive numbers already have square roots in R. It is easy to see that every element of C has a square root in C so there can be no next step.

Below, we denote by R a real closed field, $C = R[i]$ its algebraic closure and $H = R[i, j, k]$ its obvious quaternionic extension.

2.1. Theorem. *Let A be an R-algebra without zero divisors and of finite dimension over R. Then A is one of R, C, or H.*

The proof is by a sequence of steps. The claims are in italics and their proofs in roman.

1. *There is an identity in A.* Let x be a non-zero element of A. Left multiplication by x is a linear transformation of A to itself and, being injective is also surjective, so there is

an element $e \in A$ with $xe = x$.

2. *e is a left identity for A.* For any $y \in A$, we have $x(y - ey) = 0$.

3. *Every non-zero element of A has a left inverse with respect to e.* For any non-zero $x \in A$, right multiplication by x is an injective, hence surjective, linear transformation on A so there is an x' with $x'x = e$.

4. *A is a division ring.* The monoid of non-zero elements of A is a group and hence A is a real division algebra (with R in its center). We will write $1 = e$ and $x^{-1} = x'$.

5. *Assume that $dim A > 1$. Then for any $x \in A - R$, the subring $R[x]$ generated by x has dimension 2.* Since $x \notin R$, this subalgebra cannot give a subalgebra of degree 1. The powers of x can not all be linearly independent so x satisfies an irreducible polynomial equation over R. But R has no irreducible polynomial equation of degree greater than 2, so the polynomial must have degree exactly 2 and $R[x] \equiv C$. We denote by i a square root of -1 in $R[x]$ so that $R[x] = R[i]$.

Assume from here on that $A \neq R[i]$

6. *For $x \in A - R[i]$, $xi \neq ix$. Thus the function $\sigma : A \to A$ given by $\sigma(x) = ixi^{-1} = -ixi$ is an involution of A over R whose fixed field is $R[i]$.* For if $xi = ix$, then $R[i, x]$ is a commutative field of finite degree larger than 2 over R, which is not possible.

7. *Let $A' = \{x \in A \mid \sigma(x) = -x\}$. Then as a vector space, $A = A' \oplus R[i]$.* Just write

$$x = \frac{x - \sigma(x)}{2} + \frac{x + \sigma(x)}{2}$$

8. *A is 4-dimensional.* For any $x \in A'$, left multiplication by x interchanges A' and $R[i]$. Hence A' is also 2-dimensional and A has dimension 4.

9. *If $x \in A'$, then x^2 is real and negative.* Since $\sigma(x) = -x$, it is immediate that $\sigma(x^2) = x^2$ and then $x^2 \in R[i]$. Since x^2 commutes with x, it cannot have any imaginary component and is therefore real. If it were positive, then x^2 would have a square root in R, which is impossible.

10. *There is a $j \in A'$ such that $j^2 = -1$.* Take any non-zero $x \in A'$ and let $j = x/\sqrt{-x^2}$.

11. *If $k = ij$, then $k^2 = ijk = -1$.* For $k^2 = ijk = ijij = -iijj = -1$.

12. *$A = R[i, j, k]$ is the quaternions over R.*

3. Centrality of centrality.

It was central to the proof above that R be central in A. This is an example to show that the theorem may fail for the ordinary reals if $\mathbf{R}$ does not lie centrally in A. It was created, if I recall correctly, by Nathan Fine and Murray Gerstenhaber about 60 years ago when I was asked to lecture on Pontrjagin's more complicated proof of a badly stated version of the theorem above. I had to ask them if it was necessary to add the assumption that $\mathbf{R}$ lie in the center of A. It was. Whether this was an omission by Pontrjagin or the translator I have not been able to determine.

Let $S = \mathbf{R}^{\mathbf{N}}/\mathbf{u}$ where $\mathbf{u}$ is a non-principal ultrafilter on $\mathbf{N}$. Then R has cardinality $2^{\aleph_0}$ since $\mathbf{R}^{\mathbf{N}}$ does and hence transendence degree is the same. It is also real closed since that is a first order property preserved by ultrapowers. Therefore $R[i] \equiv \mathbf{C}$ and $R[i]$ contains a copy of $\mathbf{R}$ of index 2. Since the order relation on real closed fields is completely determined by the fact that the positive elements are exactly the squares, it follows that R cannot be isomorphic to $\mathbf{R}$ since R contains infinitesimals. Thus $R[i, j, k]$ is an example of a ring that contains $\mathbf{R}$ and is finite dimensional over it, but is not isomorphic to $\mathbf{H}$ since their centers are not isomorphic.