Introduction to Modern Algebra

Section 7.3. A Theorem of Frobenius—Proofs of Theorems

Lemma 7.3.1

Lemma 7.3.1. Let $\mathbb{C}$ be the field of complex numbers and suppose that the division ring D is algebraic over $\mathbb{C}$. Then $D = \mathbb{C}$.

Proof. Let $a \in D$. Since D is algebraic over $\mathbb{C}$, then by definition $a^n + \alpha_1 a^{n-1} + \cdots + \alpha_{n-1} a + \alpha_n = 0$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ (we an take the leading coefficient $\alpha_0 = 1$ without loss of generality).

Now the polynomial $p(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1} x + \alpha_n \in \mathbb{C}[x]$ can be factored in $\mathbb{C}[x]$ into a product of linear factors by Fact 1 and the Factor Theorem (see my online notes for Introduction to Modern Algebra [MATH 4127/5127] on Section IV.23. Factorizations of Polynomials; notice Corollary 23.3, "The Factor Theorem"). Therefore, $p(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n)$ where $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{C}$. Since $\mathbb{C}$ is in the center of D then every element of $\mathbb{C}$ commutes with a, and hence

$$p(a) = (a - \lambda_1)(a - \lambda_2) \cdots (a - \lambda_n) = a^n + \alpha_1 a^{n-1} + \cdots + \alpha_{n-1} a + \alpha_n = 0.$$

Lemma 7.3.1 (continued)

Lemma 7.3.1. Let $\mathbb{C}$ be the field of complex numbers and suppose that the division ring D is algebraic over $\mathbb{C}$. Then $D = \mathbb{C}$.

Proof (continued). A division ring has no zero divisors (see my Introduction to Modern Algebra notes on Section IV.19. Integral Domains; see Note 19.A), so we must have $a = \lambda_k$ for some $1 \leq k \leq n$. Since $a = \lambda_k \in \mathbb{C}$ and a is an arbitrary element of D, then we have $D \subseteq \mathbb{C}$. Since $\mathbb{C}$ is in the center of D then $\mathbb{C} \subseteq D$. Therefore $D = \mathbb{C}$, as claimed. □

Lemma 7.3.A

Lemma 7.3.A. Let division ring D be algebraic over $\mathbb{R}$ and let the center of D contain a copy of $\mathbb{C}$. Then $D = \mathbb{C}$.

Proof. Since D is algebraic over $\mathbb{R}$, then for every $a \in D$ we have $a^n + \alpha_1 a^{n-1} + \cdots + \alpha_{n-1} a + \alpha_n = 0$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{R} \subseteq \mathbb{C}$. As in the proof of Lemma 7.3.1, by Fact 1 we have

$$p(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1} x + \alpha_n = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n)$$

where $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{C}$. Since $\mathbb{C}$ is in the center of D then every element of $\mathbb{C}$ commutes with a, and hence

$$p(a) = a^n + \alpha_1 a^{n-1} + \cdots + \alpha_{n-1} a + \alpha_n = (a - \lambda_1)(a - \lambda_2) \cdots (a - \lambda_n) = 0.$$

Again as in the proof of Lemma 7.3.1, we have $a = \lambda_k \in \mathbb{C}$ for some $1 \leq k \leq n$. So $a \in \mathbb{C}$ and since a is an arbitrary element of D, then $D \subseteq \mathbb{C}$. Since $\mathbb{C}$ is in the center of D, then $\mathbb{C} \subseteq D$ and hence $D = \mathbb{C}$, as claimed. □

Theorem 7.3.1 (Frobenius)

Theorem 7.3.1. (Frobenius) Let D be a division ring algebraic over field $\mathbb{R}$, the field of real numbers. Then D is isomorphic to one of: the field of real numbers $\mathbb{R}$, the field of complex numbers $\mathbb{C}$, or the division ring of real quaternions $\mathbb{H}$.

Proof. Suppose that $D \neq \mathbb{R}$ and that $a \in D \setminus \mathbb{R}$. Since division ring D is algebraic over $\mathbb{R}$ by hypothesis, then there is some polynomial in $p(x) \in \mathbb{R}[x]$ such that $p(a) = 0$; without loss of generality we can take $p(x)$ to be irreducible in $\mathbb{R}[x]$; this follows from the fact that division ring D has no zero divisors and from Theorem 23.20 of my online notes for Introduction to Modern Algebra on Section IV.23. Factorizations of Polynomials. By Fact 2, the irreducible polynomials over $\mathbb{R}$ are of degree 1 or 2. If $p(x)$ is of degree 1, then $p(a) = 0$ implies that $a \in \mathbb{R}$, contrary to our choice of $a \in D \setminus \mathbb{R}$. So we may assume that $a^2 - 2\alpha a + \beta = 0$ for some $\alpha, \beta \in \mathbb{R}$.

Theorem 7.3.1 (Frobenius, continued 1)

Proof (continued). Next, $a^2 - 2\alpha a + \beta = 0$ implies $(a-\alpha)^2 = a^2 - 2\alpha a + \alpha^2 = \alpha^2 - \beta$. Notice that the quadratic equation allows us to solve for a in the equation $a^2 - 2\alpha a + \beta = 0$ to get $a = \dfrac{2\alpha \pm \sqrt{4\alpha^2 - 4\beta}}{2} = \alpha \pm \sqrt{\alpha^2 - \beta}$. If $\alpha^2 - \beta \geq 0$ then we have that $a \in \mathbb{R}$, contrary to our choice of $a \in D \setminus \mathbb{R}$. So it must be that $\alpha^2 - \beta < 0$, say $\alpha^2 - \beta = -\gamma^2$ where $\gamma \in \mathbb{R}$. Then $(a-\alpha)^2 = \alpha^2 - \beta = -\gamma^2$, whence $[(a-\alpha)/\gamma]^2 = -1$. Thus:

$$\text{if } a \in D \setminus \mathbb{R} \text{ then } [(a-\alpha)/\gamma]^2 = -1 \text{ for some } \alpha, \gamma \in \mathbb{R}.$$

We now consider three steps: (1) the case where D is commutative, (2) D is not commutative and we can construct a copy of the quaternions in D, and (3) D is not commutative and we show that D contains only the quaternions.

Theorem 7.3.1 (Frobenius, continued 2)

Proof (continued). Suppose D is commutative and let $a \in D \setminus \mathbb{R}$ (so we are assuming that $D \neq \mathbb{R}$ here). As shown above, there are $\alpha, \gamma \in \mathbb{R}$ such that $[(a-\alpha)/\gamma]^2 = -1$. Denote $i = (a-\alpha)/\gamma$ so that $i^2 = -1$. Since D is commutative and contains $\mathbb{R}$ and $i \in D$, then D contains the extension field $\mathbb{R}[i]$: $\mathbb{R}[i] \subseteq D$ (this is where commutativity is used). Now $\mathbb{R}[i]$ is isomorphic (as a field) to $\mathbb{C}$, so D contains an isomorphic copy of $\mathbb{C}$. Since D is algebraic over $F = \mathbb{R}$, then by Lemma 7.3.1 we have $D \cong \mathbb{C}$. Hence, if D is commutative then either $D \cong \mathbb{R}$ (in which case there is no $a \in D \setminus \mathbb{R}$) or $D \cong \mathbb{C}$ (when $a \in D \setminus \mathbb{R}$ exists). This completes step (1).

Next, suppose that D is not commutative. ASSUME that there is a in the center of D where $a \notin \mathbb{R}$. As shown above, for some $\alpha, \gamma \in \mathbb{R}$ we have $[(a-\alpha)/\gamma]^2 = -1$. But then the center of D contains $\mathbb{R}$ and contains $(a-\alpha)/\gamma$ so that the center of D contains an isomorphic copy of $\mathbb{C}$ (namely, $\mathbb{R}[(a-\alpha)/\gamma] \cong \mathbb{R}[i]$). Since a is an arbitrary non-real element of the center of D, then the center of D contains an isomorphic copy of $\mathbb{C}$.

Theorem 7.3.1 (Frobenius, continued 3)

Proof (continued). By Lemma 7.3.A, we have $D \cong \mathbb{C}$ (since D has an isomorphic copy of $\mathbb{C}$ and does not necessarily contain $\mathbb{C}$ itself, we cannot draw a conclusion of equality as given in Lemma 7.3.A, but only a conclusion of isomorphic). But if $D \cong \mathbb{C}$, then D is commutative, a CONTRADICTION to the fact that we are considering the case where D is not commutative. So the assumption that a is a non-real element of the center is false, and hence the center of D includes all of $\mathbb{R}$.

We now show that noncommutative D satisfying the hypotheses contains an isomorphic copy of the quaternions. Let $a \in D \setminus \mathbb{R}$. As shown above, for some $\alpha, \gamma \in \mathbb{R}$ we have $i = (a-\alpha)/\gamma$ satisfies $i^2 = -1$. Since $i \notin \mathbb{R}$, then i is not in the center of $\mathbb{R}$ as argued above. Therefore there is $b \in D$ such that $c = bi - ib \neq 0$. We then have

$$ic + ci = i(bi - ib) + (bi - ib)i = ibi - i^2 b + bi^2 - ibi$$

$$= ibi - (-1)b + b(-1) - ibi = 0.$$

Theorem 7.3.1 (Frobenius, continued 4)

Proof (continued). Thus $ic = -ci$, form which we have $ic^2 = (ic)c = (-ci)c = -c(ic) = -c(-ci) = c^2 i$, and so c^2 commutes with i. Since D is algebraic over $\mathbb{R}$, then $c \in D$ is the root of some polynomial in $\mathbb{R}[x]$ and we may take the polynomial to be irreducible and of degree 1 or 2 (by Fact 2). That is, $c^2 + \lambda c + \mu = 0$ for some $\lambda, \mu \in \mathbb{R}$. Since c^2 and μ commute with i, we have

$$(\lambda c)i = (-c^2 - \mu)i = -(c^2 + \mu)i = -i(c^2 + \mu) = i(-c^2 - \mu) = i(\lambda c).$$

Also, λ and i commutes (since $\lambda \in \mathbb{R}$ is in the center of D) so that $\lambda ci = i\lambda c = \lambda ic = \lambda(-ci) = -\lambda ci$. Hence $2\lambda ci = \lambda ci + \lambda ci = \lambda ci + (-\lambda ci) = 0$. Since $c \neq 0$, as shown above, and $i \neq 0$ (because, say, $i^2 = -1$) then $2ci \neq 0$; hence we must have $\lambda = 0$. Because $c^2 + \lambda c + \mu = 0$, this implies that $c^2 = -\mu$. Now $c \notin \mathbb{R}$ (because $ci = -ic \neq ic$, so c is not in the center of D), so $c^2 = -\mu$ implies that $\mu > 0$ (or else $c^2 > 0$ and c is real). With $\mu > 0$, we have $\mu = \nu^2$ for some $\nu \in \mathbb{R}$. Therefore $c^4 = -\nu^2$. Let $j = c/\nu$.

Theorem 7.3.1 (Frobenius, continued 5)

Proof (continued). Then j satisfies

1. $j^2 = c^2/\nu^2 = c^2/(-c^2) = -1$, and
2. $ji + ij = (c/\nu)i + i(c/\nu) = (ci + ic)/\nu = 0$ because $ci + ic = 0$.

Let $k = ij$. Then $k^2 = (ij)^2 = ijij = ij(-ji) = -ij^2 i = -i(-1)i = i^2 = -1$. Also, $ijk = (k)k = k^1 = -1$. We now have that $i^2 = j^2 = k^2 = ijk = -1$. Since $k = ij$, then $-k = ji$ so $jk + kj = j(ij) + (ij)j = j(-ji) + ij^2 = -(j^2)i - i = i - i = 0$ and $ki + ik = (ij)i + i(ij) = (-ji)i + i^2 j = -ji^2 - j = j - j = 0$. Now $jk = j(ij) = j(-ji) = -j^2 i = i$ and $ki = (ij)i = (-ji)i = -ji^2 = j$. We now have $ij = -ji = k$, $jk = -kj = i$, and $ki = -ik = j$. Of course we have $ri = ir$, $rj = jr$, and $rk = kr$ for all $r \in \mathbb{R}$ since the center of D includes $\mathbb{R}$. So the equations defining the quaternions are satisfied in the event that D is not commutative, and we have that D contains an isomorphic copy of the quaternions, say T. This completes step (2).

Theorem 7.3.1 (Frobenius, continued 6)

Proof (continued). Lastly, we want to show that D equals the quaternions, $\mathbb{H}$. Let $r \in D$ satisfy $r^2 = -1$ (such $r \in D$ exists as described above; for example, $i^2 = j^2 = k^2 = -1$). The normalizer of r in D is $N(r) = \{x \in D \mid xr = rx\}$ (this is an idea from group theory, but since the nonzero elements of a division ring form a multiplicative group, the idea applies here as well). In Modern Algebra 1 (MATH 5410), the normalizer of r in D is called the *centralizer* of r in the (multiplicative) group D. It is shown that this is the "stabilizer group" under the group action of conjugation; this is a group by Theorem II.4.2 of Modern Algebra 1 in Section II.4. The Action of a Group on a Set. Moreover, for $\alpha_0, \alpha_1 \in \mathbb{R}$ we have $\alpha_0 + \alpha_1 r$ is in the center of $N(r)$ because

$$\begin{aligned}(\alpha_0 + \alpha_1 r)r &= \alpha_0 r + \alpha_1 r^2 \\ &= r\alpha_0 + r\alpha_1 r \text{ because } \alpha_0, \alpha_1 \in \mathbb{R} \text{ and} \\ &\quad \mathbb{R} \text{ is in the center of } D \\ &= r(\alpha_0 + \alpha_1 r).\end{aligned}$$

Theorem 7.3.1 (Frobenius, continued 7)

Proof (continued). Since $N(r)$ is a subgroup of the multiplicative group of the division ring D, and $N(r)$ is closed under addition, then $N(r)$ is a sub-division ring of D. Since division ring D is algebraic over $\mathbb{R}$ (and hence so is division ring $N(r) \subseteq D$) and the center of $N(r)$ contains the isomorphic copy of $\mathbb{C}$ of $\{\alpha_0 + \alpha_1 r \mid \alpha_0, \alpha_1 \in \mathbb{R}, r^2 = -1\}$, then by Lemma 7.3.A (applied to $N(r)$) we have $N(r) \cong \mathbb{C}$ and so $N(r) = \{\alpha_0 + \alpha_1 r \mid \alpha_0, \alpha_1 \in \mathbb{R}\}$. Thus if $xr = rx$ where $r^2 = -1$, then $x = \alpha_0 + \alpha_1 r$ for some $\alpha_0, \alpha_1 \in \mathbb{R}$.

Let $u \in D \setminus \mathbb{R}$. As shown above, for some $\alpha, \beta \in \mathbb{R}$ we have $w = (u - \alpha)/\beta$ satisfies $w^2 = -1$. Notice that

$$i(wi + iw) = iwi + i^2 w = iwi - w = iwi + w(-1) = iwi + wi^2 = (iw + wi)i$$

so that $wi + iw$ commutes with i and $wi + iw$ is in the center of $N(i)$.

Theorem 7.3.1 (Frobenius, continued 8)

Proof (continued). Also,

$$w(wi+iw) = w^2 i + wiw = -i + wiw = i(-1) + wiw$$

$$= i(w^2) + wiw = (iw+wi)w$$

so that $wi+iw$ commutes with w and $wi+iw$ is in the center of $N(w)$. As argued above, we have (with $x = wi+iw$ and first $r = i$, then second $r = w$) that $wi+iw = \alpha_0' + \alpha_1' i = \alpha_0 + \alpha_1 w$ for $\alpha_0, \alpha_1, \alpha_0', \alpha_1' \in \mathbb{R}$. ASSUME $w \notin T$ (where T is the isomorphic copy of the quaternions in D). Then the relation $wi+iw = \alpha_0 + \alpha_1 w$ implies that $\alpha_1 = 0$ (otherwise, we have $w = (\alpha_0' - \alpha_0 + \alpha_1')/\alpha_1 \in T$). Thus $wi+iw = \alpha_0 \in \mathbb{R}$. Similarly, $wj+jw = \beta_0 \in \mathbb{R}$ and $wk+kw = \gamma_0 \in \mathbb{R}$. Define

$$z = w + \frac{\alpha_0}{2} i + \frac{\beta_0}{2} j + \frac{\gamma_0}{2} k.$$

Theorem 7.3.1 (Frobenius, continued 9)

Proof (continued). Then

$$\begin{aligned} zi+iz &= \left(w + \frac{\alpha_0}{2} i + \frac{\beta_0}{2} j + \frac{\gamma_0}{2} k\right) i + i \left(w + \frac{\alpha_0}{2} i + \frac{\beta_0}{2} j + \frac{\gamma_0}{2} k\right) \\ &= (wi+iw) + \frac{\alpha_0}{2}(i^2+i^2) + \frac{\beta_0}{2}(ji+ij) + \frac{\gamma_0}{2}(ki+ik) \\ &= \alpha_0 - \alpha_0 \text{ since } wi+iw = \alpha_0, i^2 = -1, ji_ij = 0, \text{ and } ki+ik = 0 \\ &= 0. \end{aligned}$$

Similarly, $zj+jz = 0$ and $zk+kz = 0$. We now show that $z = 0$. Since $0 = zk+kz = zij+ijz = (zi+iz_j+i(jz-zj) = i(jz-zj)$ since $zi+iz = 0$, as just shown. Now $i \neq 0$ (since $i^2 = -1$), so $jz-zj = 0$ (because a division ring has no zero divisors). But we have shown in step (2) that $jz+zj = 0$ so that we must have $2jz = 0$, and since $2j \neq 0$ then $z = 0$.

Theorem 7.3.1 (Frobenius, continued 10)

Proof (continued). From the definition of z we then have

$$z = w + \frac{\alpha_0}{2} i + \frac{\beta_0}{2} j + \frac{\gamma_0}{2} k = 0,$$

from which

$$w = -\frac{\alpha_0}{2} i - \frac{\beta_0}{2} j - \frac{\gamma_0}{2} k \in T,$$

a CONTRADICTION to the assumption that $w \notin T$. Therefore $w \in T$. Since $w = (u-\alpha)/\beta$, then $u = \beta w + \alpha$ and so $u \in T$ (because $w \in T$ and $\alpha, \beta \in \mathbb{R}$). Now u is an arbitrary element of $D \setminus \mathbb{R}$, so we have that $D \setminus \mathbb{R} \subseteq T$ and, of course, $\mathbb{R} \subseteq T$. Therefore $D \subseteq T$. In step (2) we showed that $T \subseteq D$, so we now have that $T = D$. That is, $D = T \cong \mathbb{H}$. This is step (3). □