

*Problem 1* (13.6.6). Prove that for  $n$  odd,  $n > 1$ ,  $\Phi_{2n}(x) = \Phi_n(-x)$ .

*Proof.* Begin with  $\Phi_n(-x)$ . Then we have that

$$\Phi_n(-x) = \prod_{1 \leq d < n | (d,n)=1} (-x - \zeta_n^d)$$

If we pull out the negatives we get

$$\Phi_n(-x) = (-1)^{\varphi(n)} \prod_{1 \leq d < n | (d,n)=1} (x - \zeta_n^{d+n/2})$$

Since  $\varphi(m)$  is even for  $m \geq 3$  we can safely remove it. Then we change the base of  $\zeta_n$  to get

$$\Phi_n(-x) = (-1)^{\varphi(n)} \prod_{1 \leq d < n | (d,n)=1} (x - \zeta_{2n}^{2d+n})$$

All of the  $2d + n$  are greater than or equal to 1 and less than  $2n$ . Moreover as  $n$  is odd, greater than 1, and  $\gcd(d, n) = 1$  we have that  $\gcd(2d, n) = 1$ . Since  $\deg \Phi_{2n}(x) = \varphi(2n) = \varphi(n)$  and there are  $\varphi(n)$  factors in the above product we must have all of the factors for  $\Phi_{2n}(x)$ .

Therefore

$$\Phi_n(-x) = \Phi_{2n}(x)$$

for  $n$  odd and  $n > 1$ . □

*Problem 2* (13.6.9). Suppose  $A$  is an  $n \times n$  matrix over  $\mathbb{C}$  for which  $A^k = I$  for some integer  $k \geq 1$ . Show that  $A$  can be diagonalized. Show that the matrix  $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$  where  $\alpha$  is an element of a field of characteristic  $p$  satisfies  $A^p = I$  and cannot be diagonalized if  $\alpha \neq 0$ .

*Proof.* Let  $J$  be the Jordan normal form of  $A$ . This will exist since we are working over the complex numbers. If  $J$  is diagonalizable then  $A$  will be as well. However because we have the relation  $A^k - I_n = 0$  for some  $k > 1$  it follows that the minimal polynomial of  $A$  will be  $x^k - 1$ . However this has all distinct roots. As such the block matrices in  $J$  will have to be  $1 \times 1$  since the eigenvalues are distinct. Thus  $J$  is a diagonal matrix and so is  $A$ .

For the second part first note that

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & k\alpha \\ 0 & 1 \end{pmatrix}$$

which demonstrates that  $A^p = I$  since we are in a field of characteristic  $p$ . If we calculate the minimal polynomial of  $A$  where  $\alpha \neq 0$  we get  $(x - 1)^2$ . Since the eigenvalues are not unique it will not be diagonalizable. □

*Problem 3* (13.6.10). Let  $\varphi$  denote the Frobenius map  $x \mapsto x^p$  on the finite field  $\mathbb{F}_{p^n}$ . Prove that  $\varphi$  gives an isomorphism of  $\mathbb{F}_{p^n}$  to itself. Prove that  $\varphi^n$  is the identity map and that no lower power of  $\varphi$  is the identity.

*Proof.* Since powers distribute over multiplication it is clear that  $\varphi$  preserves multiplication. The fact that it preserves addition follows from  $\mathbb{F}_{p^n}$  being of characteristic  $p$  as:

$$(x + y)^p = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} = x^p + y^p$$

Now we must show that the map is both injective and surjective. We will start with injectivity. Suppose that  $x^p = 1$ . Then

$$x^p - 1^p = (x - 1)^p = 0$$

Which implies that  $x = 1$  since we are in a field. Since the kernel is trivial it follows that  $\varphi$  is injective.

For surjectivity note that  $F_{p^n}^*$  is a multiplicative group of order  $p^n - 1$ . As such given  $y \in F_{p^n}^*$  we have that  $y^{p^n} = y$ . It then follows that

$$\left(y^{p^{n-1}}\right)^p = \varphi\left(y^{p^{n-1}}\right) = y$$

which demonstrates that  $\varphi$  is surjective.

Therefore the Frobenius map  $\varphi$  is an isomorphism.

For the latter portion note that  $\varphi^n(x) = x^{p^n}$  which is equal to  $x$  from the argument made earlier. However this cannot occur from  $m < n$ . If it did then we would have that  $x^{p^m-1} = x$  for all  $x \in \mathbb{F}_{p^n}$ . This would imply that the orders of all elements in  $\mathbb{F}_{p^n}$  is at most  $p^m - 1$ . However this is a contradiction as the multiplicative groups for finite fields are cyclic.  $\square$

*Problem 4 (13.6.13).* This exercise outlines a proof of Wedderburn's Theorem that a finite division ring  $D$  is a field.

- Let  $Z$  denote the center of  $D$ . Prove that  $Z$  is a field containing  $\mathbb{F}_p$  for some prime  $p$ . If  $Z = \mathbb{F}_q$  prove that  $D$  has order  $q^n$  for some integer  $n$ . [ $D$  is a vector space over  $Z$ ].
- The nonzero elements  $D^\times$  of  $D$  form a multiplicative group. For any  $x \in D^\times$  show that the nonzero elements of  $D$  which commute with  $x$  form a division ring which contains  $Z$ . Show that this division ring is of order  $q^m$  for some integer  $m$  and that  $m < n$  if  $x$  is not an element of  $Z$ .
- Show that the class equation for the group  $D^\times$  is

$$q^n - 1 = (q - 1) + \sum_{i=1}^r \frac{q^n - 1}{|C_{D^\times}(x_i)|}$$

where  $x_1, x_2, \dots, x_r$  are representatives of the distinct conjugacy classes in  $D^\times$  not contained in the center of  $D^\times$ . Conclude from (b) that for each  $i$ ,  $|C_{D^\times}(x_i)| = q^{m_i} - 1$  for some  $m_i < n$ .

- Prove that since  $\frac{q^n - 1}{q^{m_i} - 1}$  is an integer (namely, the index  $|D^\times : C_{D^\times}(x_i)|$ ) then  $m_i$  divides  $n$ . Conclude that  $\Phi_n(x)$  divides  $(x^n - 1)/(x^{m_i} - 1)$  and hence that the integer  $\Phi_n(q)$  divides  $(q^n - 1)/(q^{m_i} - 1)$  for  $i = 1, 2, \dots, r$ .
- Prove that (c) and (d) imply that  $\Phi_n(q) = \prod_{\zeta \text{ primitive}} (q - \zeta)$  divides  $q - 1$ . Prove that  $|q - \zeta| > q - 1$  (complex absolute value) for any root of unity  $\zeta \neq 1$  [note that 1 is the closest point on the unit circle in  $\mathbb{C}$ ] to the point  $q$  on the real line]. Conclude that  $n = 1$ , i.e., that  $D = Z$  is a field.

*Proof.* (a) Since  $D$  is a finite division ring the center  $Z$  is a commutative finite division ring. Thus  $Z$  is a field. Moreover all finite fields are of order  $p^n$  where  $p$  is a prime. If  $Z \cong \mathbb{F}_{p^n}$  then this will contain  $\mathbb{F}_p$  as a subfield as  $\mathbb{F}_{p^n}$  is the splitting field for  $x^{p^n} - x$  over  $\mathbb{F}_p$ .

For the second part suppose that  $Z \cong \mathbb{F}_q$ . Let  $b_1 := 1$ . Then together define  $\mathcal{B}_i := \text{span}\{b_1, \dots, b_i\}$  (linear combinations with coefficients in  $Z$ ) and  $b_{i+1}$  to be some element in  $D \setminus \mathcal{B}_i$ . Since  $D$  is finite it follows that there will exist an  $n$  where  $\mathcal{B}_n = D$ . Now we will show that the set  $\{b_1, \dots, b_n\}$  forms a basis for  $D$ . Since it already spans  $D$  we just need to show that it is linearly independent.

Suppose otherwise. Then we have a nontrivial linear combination  $\sum_0^n a_i b_i = 0$  giving us that  $-\frac{1}{a_n} \sum_0^{n-1} a_i b_i = b_n$ . However this contradicts the assumption that  $b_n \in D \setminus \mathcal{B}_{n-1}$ .

Therefore  $\{b_1, \dots, b_n\}$  forms a basis for  $D$  over  $Z$  and as such  $|D| = q^n$  for some positive integer  $n$ .

- (b) Let  $x \in D^\times$  and let  $D_x$  be the set of elements that commute with  $x$ . We will show that  $D_x$  is a division ring and that  $Z \subseteq D_x$ . Since elements of the center commute with all elements of  $D$  it is clear that  $Z \subseteq D_x$ . This implies that 0 and 1 are in  $D_x$ .

Next we show that  $D_x$  is closed under addition, multiplication, and inverses. Let  $r, s \in D_x$ . Then for addition we have

$$(r + s)x = rx + sx = xr + xs = x(r + s)$$

For multiplication we have

$$(rs)x = r(sx) = r(xs) = (rx)s = (xr)s = x(rs)$$

Finally for inverses since we have  $rx = xr$  for  $r \in D_x$  if we multiply on the left and right by  $r^{-1}$  it follows that

$$xr^{-1} = r^{-1}x$$

implying that  $r^{-1} \in D_x$  whenever  $r \in D_x$ .

Therefore  $D_x$  is a finite division ring. Moreover it fulfills the same hypothesis as in part (a) so it must be of size  $q^m$  for some  $m$ . If  $x \notin Z$  then there is some element  $y \in D$  such that  $yx \neq xy$ . Then  $y \notin D_x$ . However since both  $D$  and  $D_x$  are vector spaces over  $Z$  with size  $q^n$  and  $q^m$  respectively it must be that  $n > m$  since  $D_x$  is a strict subset of  $D$ .

- (c) Let  $D^\times$  act on itself by conjugation. Then the class equation for  $D^\times$  will be

$$|D^\times| = |Z| + \sum_1^r \frac{|D^\times|}{|C_{D^\times}(x_i)|}$$

If we substitute in for known values we get that

$$q^n - 1 = (q - 1) + \sum_1^r \frac{q^n - 1}{|C_{D^\times}(x_i)|}$$

Note that the stabilizer for each  $x_i$  will in fact be  $D_{x_i}$  from part (c). As such the order will be  $q^{m_i} - 1$  where  $m_i < n$  as  $x_i \notin Z$ .

(d) From class we have the formula

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Applying that formula here we can rewrite the quotient as

$$\frac{q^n - 1}{q^{m_i} - 1} = \frac{\prod_{d|n} \Phi_d(q)}{\prod_{d'|m_i} \Phi_{d'}(q)} \in \mathbb{Z}$$

However since this is an integer we must have that each term  $\Phi_{d'}(q)$  divides evenly into the above which implies that  $d'|n$ . Since  $m_i|m_i$  we have that  $m_i|n$ .

Moreover if we replace  $q$  with  $x$  the result still holds. It then follows since  $\Phi_n(x)|(x^n - 1)$  as  $m_i < n$  so it will not be canceled. Thus  $\Phi_n(q) | \frac{q^n - 1}{q^{m_i} - 1}$ .

(e) From (d) we have that  $\Phi_n(q)$  divides  $q^n - 1$  and that it divides  $\frac{q^n - 1}{q^{m_i} - 1}$  for each  $i$ . Thus from the class equation in part (c) it must be the case that  $\Phi_n(q)$  also divides  $q - 1$ .

Now we will show that  $|q - \zeta| > q - 1$  if  $\zeta \neq 1$ . If we evaluate  $|q - \zeta|^2$  we get

$$|q - \zeta|^2 = (q - \cos \theta)^2 + (-\sin \theta)^2 = q^2 + 1 - 2q \cos \theta$$

Then if we compare this to  $(q - 1)^2$  we see that

$$q^2 + 1 - 2q \cos \theta \geq q^2 - 1 - 2q$$

and since  $\zeta \neq 1$  we have that  $\cos \theta < 1$  which makes this inequality strict. Thus  $n = 1$  which implies that  $Z = D$  and that  $D$  is in fact a field. □

*Problem 5 (14.1.4).* Prove that  $\mathbb{Q}[\sqrt{2}]$  and  $\mathbb{Q}[\sqrt{3}]$  are not isomorphic.

*Proof.* Suppose that  $\mathbb{Q}[\sqrt{2}]$  and  $\mathbb{Q}[\sqrt{3}]$  were isomorphic. Then there would be an isomorphism  $\varphi : \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{3}]$ . Let  $\varphi(\sqrt{2}) = a + b\sqrt{3}$ . Then we have that

$$\varphi(2) = \varphi(1 + 1) = \varphi(1) + \varphi(1) = 2$$

it then follows that  $(a + b\sqrt{3})^2 = 2$ . However by expanding we get

$$a^2 + 3b^2 + 2ab\sqrt{3} = 2$$

which implies that either  $a$  or  $b$  is zero since we are in a field. If  $b = 0$  then  $a^2 = 2$  which implies that  $\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$  which is a contradiction. On the other hand if  $a = 0$  then  $b^2 = 2/3$  which implies that  $\sqrt{3}b = \sqrt{2}$ . Then  $\sqrt{2}/3 \in \mathbb{Q}[\sqrt{3}]$  once again which is a contradiction.

Therefore the fields  $\mathbb{Q}[\sqrt{2}]$  and  $\mathbb{Q}[\sqrt{3}]$  are not isomorphic. □

*Problem 6 (14.2.4).* Let  $p$  be a prime. Determine the elements of the Galois group of  $x^p - 2$ .

*Proof.* □

*Problem 7* (14.2.5). Prove that the Galois group of  $x^p - 2$  for  $p$  a prime is isomorphic to the group of matrices  $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$  where  $a, b \in \mathbb{F}_p, a \neq 0$ .

*Proof.*

□

*Problem 8* (14.2.14). Show that  $\mathbb{Q}(\sqrt{2} + \sqrt{2})$  is a cyclic quartic field, i.e., is a Galois extension of degree 4 with cyclic Galois group.

*Proof.* For the sake of brevity let  $\alpha := \sqrt{2} + \sqrt{2}$ . We know from a prior homework that the degree of  $\mathbb{Q}(\alpha)$  is 4. We also know that minimal polynomial for  $\alpha$  is  $x^4 - 4x^2 + 2$  whose roots are  $\pm\sqrt{2} \pm \sqrt{2}$ . Thus the Galois group for this field must be of size 4. Define  $\sigma : \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}(\alpha)$  by its action on the roots

$$\alpha \mapsto \alpha^3 - \alpha, \quad -\alpha \mapsto -\alpha^3 + \alpha, \quad \alpha^3 - \alpha \mapsto -\alpha, \quad -\alpha^3 + \alpha \mapsto \alpha$$

**Probably want to justify why this is a homomorphism at all**

This is of order 4. As such the Galois group must be isomorphic to  $\mathbb{Z}_4$ .

□