Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

December 5, 2020

Problems in Section 5.3.

1. In the proof of Lemma 5.3.1, prove that the degree of $q(x)$ is one less than that of $p(x)$.

Proof. Assuming $p(x)$ as a polynomial in $K[x]$. Then from $p(x) = (x-b)q(x)+p(b)$ implies that

$$\deg(p(x)) = \deg((x-b)q(x) + p(b)) = \deg((x-b)q(x)) = \deg(x-b) + \deg(q(x))$$

in $K[x]$. But since $\deg(x-b) = 1$, $\deg(q(x))$ is exactly one less than $\deg(p(x))$. □

2. In the proof of Theorem 5.3.1, prove in all detail that the elements $1+V, x+V, \cdots, x^{n-1}+V$ form a basis of E over F.

Proof. Refer the Problem 2, Section 5.1. □

3. Prove Lemma 5.3.3 in all detail.

Proof. We prove that the mapping $\tau^* : F[x] \to F'[t]$ defined by

$$f(x)\tau^* = (a_0 + a_1 x + \cdots a_n x^n)\tau^* = (a_0\tau) + (a_1\tau)t + \cdots (a_n\tau)t^n$$

where $\tau : F \to F'$ is an onto isomorphism. Choose $f(x), g(x) \in F[x]$ where

$$f(x) = a_0 + a_1 x + \cdots a_n x^n,$$
$$g(x) = b_0 + b_1 x + \cdots b_m x^m.$$

Observe that

$$\begin{aligned}(f(x) + g(x))\tau^* &= \left(\sum_{i=0}^{k} c_i x^i\right)\tau^* = \sum_{i=0}^{k}(c_i\tau)t^i \\ &= \sum_{i=0}^{k}(a_i + b_i)\tau t^i = \sum_{i=0}^{k}(a_i\tau + b_i\tau)t^i \\ &= \sum_{i=0}^{k}(a_i\tau)t^i + \sum_{i=0}^{k}(b_i\tau)t^i = f(x)\tau^* + g(x)\tau^*\end{aligned}$$

and by denoting $d_i = \sum_{j=0}^{i} a_j b_{i-j}$, $f(x)g(x) = \sum_{i=0}^{l} d_i x^i$,

$$\begin{aligned}
(f(x)g(x))\tau^* &= \left(\sum_{i=0}^{l} d_i x^i\right)\tau^* = \sum_{i=0}^{l}(d_i\tau)t^i \\
&= \sum_{i=0}^{l}\left(\sum_{j=0}^{i} a_j b_{i-j}\right)\tau t^i \\
&= \sum_{i=0}^{l}\left(\sum_{j=0}^{i}(a_j\tau)(b_{i-j}\tau)\right)t^i = f(x)\tau^* \cdot g(x)\tau^*.
\end{aligned}$$

Thus, τ^* is a homomorphism. Recall the fact that two polynomials are equal if and only if their coefficients are componentwise equal. Now since τ is an onto isomorphism, the bijectivity of τ^* follows. Therefore, τ^* is an isomorphism of $F[x]$ onto $F'[t]$. □

4. Show that τ^{**} in Lemma 5.3.4 is well defined and is an isomorphism of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$.

Proof. We prove that the mapping $\tau^{**} : F[x]/(f(x)) \to F'[t]/(f'(t))$ defined by

$$(g(x) + (f(x))\tau^{**} = g'(t) + (f'(t))$$

is a well defined onto isomorphism. Choose $g(x), h(x)$ such that $g(x) + (f(x)) = h(x) + (f(x))$. That is, $g(x) - h(x) = p(x)f(x)$ for some $p(x) \in F[x]$. Then if follows that $g'(t) - h'(t) = p'(t)f'(t)$ so that $g'(t) + (f'(t)) = h'(t) + (f'(t))$. Hence, τ^{**} is well defined. Now we show that τ^{**} is a homomorphism. Observe that

$$\begin{aligned}
\left((g(x) + (f(x))) + (h(x) + (f(x)))\right)\tau^{**} &= (g(x) + h(x) + (f(x)))\tau^{**} \\
&= g'(t) + h'(t) + (f'(t)) \\
&= (g'(t) + (f'(t))) + (h'(t) + (f'(t))) \\
&= (g(x) + (f(x))\tau^{**} + (h(x) + (f(x))\tau^{**}
\end{aligned}$$

and

$$\begin{aligned}
\left((g(x) + (f(x))) \cdot (h(x) + (f(x)))\right)\tau^{**} &= (g(x)h(x) + (f(x))\tau^{**} \\
&= g'(t)h'(t) + (f'(t)) \\
&= (g'(t) + (f'(t))) \cdot (h'(t) + (f'(t))) \\
&= (g(x) + (f(x)))\tau^{**} \cdot (h(x) + (f(x)))\tau^{**}
\end{aligned}$$

so that τ^{**} is a homomorphism. From the fact that $g(x)\tau^* = g'(t)$ and τ^* being an onto isomorphism(Problem 3), the bijectivity of τ^{**} follows. Therefore, τ^{**} is a well defined onto isomorphism between $F[x]/(f(x))$ and $F'[t]/(f'(t))$. □

5. In Example 3 at the end of this section prove that $F(w)$ is the splitting field of x^4+x^2+1.

Proof. Observe that

$$f(x) = x^4 + x^2 + 1 = (x - w)(x + w)(x - w^2)(x + w^2)$$

so that $f(x)$ splits over F in $F(w)$. $F(w)$ is the splitting field of $f(x)$ over F. $\square$

6. Let F be the field of rational numbers. Determine the degrees of the splitting fields of the following polynomials over F.
a) $x^4 + 1$.

Solution. Let $\zeta = e^{\frac{i\pi}{4}}$. We see that

$$f(x) = x^4 + 1 = (x - \zeta)(x + \zeta)(x - \zeta^3)(x + \zeta^3)$$

so that $F(\zeta)$ is the splitting field of $f(x)$ over F. Note that $x^4 + 1$ is irreducible over $F = \mathbb{Q}$(take $x = x + 1$ and apply Eisenstein Criterion). Therefore, $F(\zeta)$ is extension field of F of degree 4. $\square$

b) $x^6 + 1$.

Solution. Note that $f(x) = x^6 + 1$ has 6 distinct roots $e^{i\left(\frac{\pi k}{3}+\frac{\pi}{6}\right)}$, $k = 0, 1, \cdots, 5$, so that $f(x)$ splits over $F(\zeta)$ where $\zeta = e^{\frac{i\pi}{6}}$. Moreover, for $g(x) = x^4 - x^2 + 1$, $g(\zeta) = 0$. Since $g(x)$ being irreducible in $F = \mathbb{Q}$, $[F(\zeta), F] = 4$. Therefore, $F(\zeta)$ is the splitting field of $f(x)$ over F with degree 4. $\square$

c) $x^4 - 2$.

Solution. Observe that

$$f(x) = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$$

so that $E = F(\sqrt[4]{2}, i)$ is the splitting field of $f(x)$ over F. Note that $x^2 + 1$ still being irreducible in $F(\sqrt[4]{2})$, $[E : F(\sqrt[4]{2})] = 2$. Moreover, $[F(\sqrt[4]{2}), F] = 4$. Therefore, the degree of E over F is $[E : F] = [E : F(\sqrt[4]{2})][F(\sqrt[4]{2}), F] = 8$. $\square$

d) $x^5 - 1$.

Solution. Let $\zeta = e^{\frac{i2\pi}{5}}$. Observe that

$$f(x) = x^5 - 1 = (x - \zeta)(x - \zeta^2)(x - \zeta^3)(x - \zeta^4)(x - \zeta^5)$$

so that $F(\zeta)$ is the splitting field of $f(x)$ over F. Since ζ is a root of $g(x) = x^4+x^3+x^2+x+1$ and $g(x)$ being irreducible in $F = \mathbb{Q}$, $[F(\zeta) : F] = 4$. $\square$

e) $x^6 + x^3 + 1$.

Solution. Let $\zeta = e^{\frac{i2\pi}{9}}$. Observe that

$$f(x) = x^6 + x^3 + 1 = (x - \zeta)(x + \zeta)(x - \zeta^4)(x + \zeta^4)(x - \zeta^7)(x - \zeta^7)$$

so that $F(\zeta)$ is the splitting field of $f(x)$ over F. Since $x^6 + x^3 + 1$ is irreducible over $F = \mathbb{Q}$, $[F(\zeta) : F] = 6$. □

7. If p is a prime number, prove that the splitting field over F, the field of rational numbers, of the polynomial $x^p - 1$ is of degree $p - 1$.

Proof. Let $\zeta = e^{\frac{i2\pi}{7}}$, the standard primitive root of unity p. Thence, $f(x) = x^p - 1$ has p distinct roots $1, \zeta, \zeta^2, \cdots, \zeta^{p-1}$. Thus, $F(\zeta)$ is the splitting field of $f(x)$ over F. Let $g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Then $g(\zeta) = 0$ clearly. But from the Problem 3, Section 3.10, $g(x)$ is irreducible over rationals. Therefore, $[F(\zeta) : F] = p - 1$. □

8. If $n > 1$, prove that the splitting field of $x^n - 1$ over the field of rational numbers is of degree $\Phi(n)$ where Φ is the Euler Φ-function.

Proof. Let w denote the standard primitive nth root of unity. Since

$$x^n - 1 = (x - w)(x - w^2) \cdots (x - w^{n-1})(x - w^n)$$

we know that the splitting field of $x^n - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(w)$. To show that $[\mathbb{Q}(w) : \mathbb{Q}] = \Phi(n)$, we claim that the nth Cyclotomic polynomial $\phi_n(x)$ which has degree $\Phi(n)$, is satisfied by w and irreducible in $\mathbb{Q}$.

Definition (nth Cyclotimic Polynomial). For any positive integer n, the nth Cyclotomic polynomial $\phi_n(x)$ is given by

$$\phi_n(x) = (x - w_1)(x - w_2) \cdots (x - w_s)$$

where $w_1, w_2, \cdots, w_s$ are primitive nth roots of unity.

Clearly from the definition, $\phi_n(x)$ is monic. Further, we know that there are $\Phi(n)$ many primitive nth roots of unity for n. Hence, $\deg \phi_n(x) = \Phi(n)$. Now we prove an useful Lemma:

Lemma. (A). Let n be a positive integer. Then

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

($\Rightarrow$) Suppose w is a root of $\phi_d(x)$ where $d \mid n$. That is, w is a primitive dth root of unity. Let q be the integer such that $dq = n$. Thus, $w^n = (w^d)^q = 1$ so that w is a root of $x^n - 1$. Now we suppose w is a root of $x^n - 1$. Then w is a nth root of unity. Let d denote the order of w. Equivalently, $w^d = 1$ so that w is a root of $\phi_d(x)$. As it is must that $d \mid n$ and hence, we conclude that $x^n - 1$ and $\prod_{d|n} \phi_d(x)$ share all their roots. As both polynomials are monic, $x^n - 1 = \prod_{d|n} \phi_d(x)$.

Lemma. (B). For any positive integer n, $\phi_n(x) \in \mathbb{Z}[x]$.

($\Rightarrow$) We make induction on n. If $n = 1$, it is trivial. Suppose we assume the given statement is true for all $k < n$. That is, $\phi_k(x) \in \mathbb{Z}[x]$ for all $k < n$. Now from Lemma (A), we know that $x^n - 1 = \prod_{d|n} \phi_d(x)$. Let $f(x) = \prod_{d|n, d<n} \phi_d(x)$. By the induction hypothesis, $f(x)$ is in $\mathbb{Z}[x]$ and monic. Assuming $x^n - 1, f(x)$ as the polynomials in $\mathbb{Q}[x]$, by the division algorithm we have

$$x^n - 1 = f(x)q(x) + r(x) = f(x)\phi_n(x),$$

where $q(x), r(x) \in \mathbb{Q}[x], \deg r(x) < \deg f(x)$. By the uniqueness of quotient and remainder, $q(x) = \phi_n(x)$ and hence $\phi_n(x) \in \mathbb{Q}[x]$. Note that both $x^n - 1$ and $f(x)$ are monic in $\mathbb{Z}[x]$. Hence, by Gauss' Lemma, $\phi_n(x) \in \mathbb{Z}[x]$.

Now we prove the irreducibility of $\phi_n(x)$ over $\mathbb{Z}$(so that in $\mathbb{Q}$).

Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible factor of $\phi_n(x)$. As $\phi_n(x)$ divides $x^n - 1$ in $\mathbb{Z}[x]$, there exists $g(x) \in \mathbb{Z}[x]$ such that $f(x)g(x) = x^n - 1$. Let w be a primitive nth root of unity, which is a zero of $f(x)$. Let p a prime such that $p \nmid n$. Thus, $(p, n) = 1$ and hence, w^p is also a primitive nth root of unity. Hence $(w^p)n - 1 = 0 = f(w^p)g(w^p)$ so that w^p is a root of either $f(x)$ or $g(x)$.
Suppose $f(w^p) \neq 0$. This forces $g(w^p) = 0$ and hence, w is a root of $g(x^p)$. Since $f(x)$ is a monic irreducible polynomial in $\mathbb{Q}[x]$, it is the minimal polynomial of w in $\mathbb{Q}[x]$. As $\mathbb{Q}[x]$ is a Principal Ideal Domain, $f(x) \mid g(x^p)$ in $\mathbb{Q}[x]$. Moreover, as $f(x)$ is monic, by Gauss Lemma, $f(x) \mid g(x^p)$ in $\mathbb{Z}[x]$. Say $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Let $\overline{g}(x), \overline{f}(x), \overline{h}(x)$ denote the polynomials in $\mathbb{Z}_p[x]$ with each coefficients reduced by modulo p. Hence, $\overline{g}(x^p) = \overline{h}(x)\overline{h}(x)$. Consequently, $(\overline{g}(x))^p = \overline{h}(x)\overline{f}(x)$. From the fact that $\mathbb{Z}_p[x]$ is an Unique Factorization Domain, $\overline{g}(x)$ and $\overline{f}(x)$ has a common irreducible factor $k(x)$. Thus, $\overline{f}(x) = m_1(x)k(x)$ and $\overline{g}(x) = m_2(x)k(x)$ for some $m_1(x), m_2(x) \in \mathbb{Z}_p[x]$. Consequently, $x^n - 1 = \overline{f}(x)\overline{g}(x) = (k(x))^2 m_1(x)m_2(x)$ in $\mathbb{Z}_p[x]$ so that $x^n - 1$ has a multiple root in some extension of $\mathbb{Z}_p$. As $\mathbb{Z}_p$ is a field of characteristic p, $x^n - 1$ must be a polynomial of form $t(x^p)$. But since $p \nmid n$, it is impossible. So this contradicts the fact that $x^n - 1$ has multiple root; hence $f(w^p) = 0$. Thus, w^p is a root of $f(x)$.
Let ζ be an arbitrary primitive nth root of unity. It is must that $\zeta \in (w)$ so that $\zeta = w^k$ for some positive integer k such that $(k, n) = 1$. Considering the prime factorization of

k, let $k = p_1^{i_1} p_2^{i_2} \cdots p_s^{i_s}$ where each $p_j \nmid n$. Recall that w^p is also a root of $f(x)$ for every prime $p \nmid n$. So does $w^k = \zeta$; ζ is a root of $f(x)$. Consequently, $f(x)$ and $\phi_n(x)$ shares all their roots. Both being monic in $\mathbb{Z}[x]$, $f(x) = \phi_n(x)$. Therefore, $\phi_n(x)$ is irreducible in $\mathbb{Z}[x]$.

Ultimately, if w denote the standard primitive nth root of unity, $\phi_n(w) = 0$ and with the fact that $\deg \phi_n(x) = \Phi(n)$, we have $[\mathbb{Q}(w) : \mathbb{Q}] = \Phi(n)$.

□

9. If F is the field of rational numbers, find necessary and sufficient conditions on a and b so that the splitting field of $x^3 + ax + b$ has degree exactly 3 over F.

Proof. First we prove that $f(x) = x^3 + ax + b$ must be irreducible in order to have splitting field of degree 3. Suppose $f(x)$ was reducible, then $f(x)$ has $\alpha \in \mathbb{Q}$ as a root so that the degree of the splitting field is less or equal to 2. Thus, $f(x)$ is irreducible in Q. Moreover, $f(x)$ can have either three of the following:

- $f(x)$ has multiple roots,
- $f(x)$ has one real and two non-real roots,
- $f(x)$ has three distinct real roots.

First note that $f(x)$ cannot have multiple roots since it is irreducible. Suppose $f(x)$ has now a complex root w and non-rational real root α. As $w \notin \mathbb{Q}(\alpha)$, the degree of splitting field must exceed 3, so that a contradiction. So, there is only one choice left, that is, $f(x)$ has three distinct real roots. i.e.,

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma),$$

where $\alpha, \beta, \gamma \in \mathbb{R} - \mathbb{Q}$ are all distinct. Now by Viete's theorem,

$$\begin{aligned} &\alpha + \beta + \gamma = 0, \\ &\alpha\beta + \beta\gamma + \gamma\alpha = a, \\ &\alpha\beta\gamma = b. \end{aligned}$$

For $f(x)$ to have splitting field E of degree 3 over F, it is must that $\beta, \gamma \in \mathbb{Q}(\alpha)$. From above, we can find that $\beta + \gamma = -\alpha$, $\beta\gamma = -b/\alpha = \alpha^2 + a$ so that the polynomial $g(t)$

$$g(t) = t^2 + \alpha t + (\alpha^2 + a) \in \mathbb{Q}(\alpha)[t]$$

is the polynomial having β and γ as root. Note that $\beta, \gamma \in \mathbb{Q}(\alpha)$ if and only if the discriminant $\alpha^2 - 4(\alpha^2 + a) = -3\alpha^2 - 4a$ is a square in $\mathbb{Q}(\alpha)$. □

10. Let p be a prime number and let $F = J_p$, the field of integers mod p.
a) Prove that there is an irreducible polynomial of degree 2 over F.

Proof. Using the fact that $f(x) = x^2+1$ is irreducible in $J_p, p = 4k+3$ and $g(x) = x^2+x+1$ is irreducible in $J_p, p = 4k+1$, there always exists irreducible polynomial of degree 2 over F. □

b) Use this polynomial to construct a field with p^2 elements.

Solution. Taking $f(x)$ defined as

$$f(x) = \begin{cases} x^2+1, & \text{if } p = 4k+3 \\ x^2+x+1, & \text{if } p = 4k+1 \end{cases}$$

then $J_p/(f(x))$ is a field with p^2 elements. □

c) Prove that any two irreducible polynomials of degree 2 over F lead to isomorphic fields with p^2 elements.

Proof. It is enough to show that any fields of p^2 elements are isomorphic. Each irreducible polynomials of degree 2 over F leads to field of p^2 elements. Denote one of them as F^*, where $|F^*| = p^2$. Since every finite field of order p^n has $F_p \simeq Z_p$ as its subfield, $f(x) = x^{p^2} - x \in F_p[x]$ is a polynomial with at most p^2 elements. But we know that $f(x)$ has distinct roots and $f(a) = 0$ for all $a \in F^*$, F^* is the splitting field of $f(x)$ over F_p. Since splitting fields of a polynomial over a given field must be unique(upto isomorphism), we are done. □

11. If E is an extension of F and if $f(x) \in F[x]$ and if ϕ is an automorphism of E leaving every element of F fixed, prove that ϕ must take a root of $f(x)$ lying in E into a root of $f(x)$ in E.

Proof. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$. Observe that

$$\begin{aligned}(f(a))\phi &= (a_0 + a_1a + \cdots a_na^n)\phi \\ &= a_0\phi + (a_1\phi)(a\phi) + \cdots + (a_n\phi)(a\phi)^n \\ &= f(a\phi)\end{aligned}$$

so that if $f(a) = 0$ for some root $a \in E$, then $0 = (f(a))\phi = f(a\phi)$. Hence $a\phi \in E$ is a root of $f(x)$ in E. □

12. Prove that $F(\sqrt[3]{2})$, where F is the field of rational numbers, has no automorphisms other than the identity automorphism.

Proof. We first prove that automorphism σ in $F(\sqrt[3]{2})$ fixes $\mathbb{Q} = F$. It is clear that $\sigma(1) = 1$. Thus, for a positive integer n,

$$\sigma(n) = \sigma(n \cdot 1) = \underbrace{\sigma(1) + \sigma(1) + \cdots + \sigma(1)}_{n \text{ times}} = n.$$

This also holds for negative integer since $\sigma(-n) = \sigma(-1 \cdot n) = \sigma(-1)n = -n$. Now consider the reciprocal $\frac{1}{m}$, where $m > 0 \in \mathbb{Z}$. Then we have

$$\begin{aligned} \sigma(1) &= \sigma \underbrace{\left(\frac{1}{m} + \frac{1}{m} + \cdots + \frac{1}{m}\right)}_{m \text{ times}} \\ &= \underbrace{\sigma\left(\frac{1}{m}\right) + \sigma\left(\frac{1}{m}\right) + \cdots + \sigma\left(\frac{1}{m}\right)}_{m \text{ times}} = m\sigma\left(\frac{1}{m}\right) \end{aligned}$$

so that $\sigma\left(\frac{1}{m}\right) = \frac{1}{m}$. Combining the results, we have that $\sigma\left(\frac{n}{m}\right) = \frac{n}{m}$. Thus, σ fixes $\mathbb{Q}$. Now, we have that $2 = \sigma(2) = \sigma(\sqrt[3]{2}^3) = \sigma(\sqrt[3]{2})^3$ so that $\sigma(\sqrt[3]{2})$, in the subfield of $\mathbb{R}$, is must that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Since any element in $F(\sqrt[3]{2})$ is the form of $a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2$,

$$\sigma(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2) = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2$$

so that $\sigma = id$, an identity automorphism. □

13. Using the result of Problem 11, prove that if the complex number α is a root of the polynomial $p(x)$ having real coefficients then $\overline{\alpha}$, the complex conjugate of α, is also a root of $p(x)$.

Proof. Let $\sigma : \mathbb{C} \to \mathbb{C}$ be a mapping defined by $\sigma(a + bi) = a - bi$, where $a, b \in \mathbb{R}$. As σ fixes the real part of the complex number and with its automorphic nature, $\sigma(\alpha) = \overline{\alpha}$ is also a root of $p(x)$. □

14. Using the result of Problem 11, prove that if m is an integer which is not a perfect square and if $\alpha + \beta\sqrt{m}$ (α, β rational) is the root of a polynomial $p(x)$ having rational coefficients, then $\alpha - \beta\sqrt{m}$ is also a root of $p(x)$.

Proof. Consider the extension field $\mathbb{Q}(\sqrt{m})$. Since it has degree 2 over $\mathbb{Q}$, every element of $\mathbb{Q}(\sqrt{m})$ is the form of $x + y\sqrt{m}$ where $x, y \in \mathbb{Q}$. Note that in any field containing $\mathbb{Q}$, its automorphism must fix the rationals. Let $\sigma : \mathbb{Q}(\sqrt{m}) \to \mathbb{Q}(\sqrt{m})$ defined by $\sigma(x + y\sqrt{m}) = x - y\sqrt{m}$. Clearly σ is an automorphism. Therefore, if $\alpha + \beta\sqrt{m}$ is a root of $p(x) \in \mathbb{Q}[x]$, $\sigma(\alpha + \beta\sqrt{m}) = \alpha - \beta\sqrt{m}$ is also a root of $p(x)$. □

15. If F is the field of real numbers, prove that if ϕ is an automorphism of F, then ϕ leaves every element of F fixed.

Proof. Let ϕ be an automorphism of F. Then it must send positive to positive, as for any $x > 0 \in \mathbb{R}$, there exists y such that $x = y^2$ and hence $\phi(x) = \phi(y^2) > 0$. Thus, ϕ preserves the order(increasing). For the sake of contradiction, if there is $x \in \mathbb{R}$ such that $\phi(x) \neq x$, then, WLOG, we can assume that $x < \phi(x)$. Moreover, we can find $q \in \mathbb{Q}$ such that $x < q < \phi(x)$. But this implies that $\phi(x) < \phi(q) = q < \phi(x)$, which is a contradiction. Therefore, ϕ must be an identity map. □

16. a) Find all real quaternions $t = a_0 + a_1 i + a_2 j + a_3 k$ satisfying $t^2 = -1$.

Proof. By simple calculation,

$$\begin{aligned} t^2 = -1 &\iff (a_0^2 - a_1^2 - a_2^2 - a_3^2) + (2a_0a_1)i + (2a_0a_2)j + (2a_0a_3)k = -1 \\ &\iff a_0 = 0, \quad a_1^2 + a_2^2 + a_3^2 = 1. \end{aligned}$$

Hence, $t = a_0 + a_1 i + a_2 j + a_3 k$ satisfies $t^2 = -1$ if and only if $a_0 = 0, a_1^2 + a_2^2 + a_3^2 = 1$. □

b) For a t as in part a) prove we can find a real quaternion s such that $sts^{-1} = i$.

Proof. Let $t = -i$ and $s = j$. Then $j(-i)(-j) = i$. □