

Tutorial 9

1. (i) Let R be a principal ideal domain and I an ideal in R . Suppose that $\pi \in I$ is an irreducible element of R . Prove that if $I \neq R$, $I = \pi R$.
- (ii) Let $\omega = e^{2\pi i/7} \in \mathbb{C}$, and let $\rho: \mathbb{Q}[x] \rightarrow \mathbb{C}$ be the evaluation homomorphism determined by $x \mapsto \omega$. Find a polynomial $p(x) \in \mathbb{Q}[x]$ that generates the ideal $\ker \rho$. Hint: part (i) and a corollary of Eisenstein's Criterion from lectures will be relevant

Solution.

- (i) Since R is a PID there is an $a \in R$ such that $I = aR$. Since $\pi \in I$ it follows that $p = ab$ for some $b \in R$. So $a|\pi$, and since π is irreducible a is either a unit or an associate of π . If a is a unit then we know $aR = R$. So a is an associate of π . So a and π generate the same principal ideal. So $\pi R = aR = I$.
 - (ii) Since $\sum_{i=0}^6 \omega^i = \frac{1-\omega^7}{1-\omega} = 0$ (by the formula for the sum of a geometric series) we see that ω is a root of the polynomial $p(x) = 1+x+x^2+x^3+x^4+x^5+x^6$. So $p(x)$ is in the ideal $\ker \rho$. The result from lectures that the question refers to is also the example on p. 65 of the course notes; we apply it here for the prime $p = 7$. It says that $p(x)$ is irreducible over \mathbb{Q} . So Part (i) tells us that either $\ker \rho = p(x)\mathbb{Q}[x]$ —that is, $p(x)$ generates $\ker \rho$ —or else $\ker \rho = \mathbb{Q}[x]$. But clearly $\ker \rho \neq \mathbb{Q}[x]$, as the polynomial 1 (for example) does not evaluate to 0 at $x = \omega$.
2. Let $\alpha = \sqrt[7]{2} \in \mathbb{R}$, and let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α ; that is, $f(x)$ is the least degree monic polynomial in $\mathbb{Q}[x]$ such that $f(\alpha) = 0$.
 - (i) Prove that $f(x)$ is a divisor of every $g(x) \in \mathbb{Q}[x]$ such that $g(\alpha) = 0$. (Hint: $g(x) = q(x)f(x) + r(x)$ for some polynomial $r(x)$ of degree less than $\deg f(x)$.)
 - (ii) Use Eisenstein's Criterion to prove that $x^7 - 2 \in \mathbb{Q}[x]$ is irreducible.
 - (iii) Deduce that $f(x) = x^7 - 2$.
 - (iv) Considering \mathbb{R} as a vector space over \mathbb{Q} , prove that the seven elements α^i with $0 \leq i \leq 6$ are linearly independent.
 - (v) Prove that the seven dimensional \mathbb{Q} -subspace E of \mathbb{R} spanned by the powers of α is in fact a subfield of \mathbb{R} .
 - (vi) Express the inverse of $\alpha^2 + 1$ as a \mathbb{Q} -linear combination of powers of α .

Solution.

For Part (ii), Eisenstein's criterion applies with $p = 2$, since the leading coefficient of $x^7 - 2$ is odd, all the other coefficients are even, and the constant coefficient is not divisible by 4. So $x^7 - 2$ is irreducible over \mathbb{Q} . The proofs of Parts (i) and (iii) are given in the solution to Question 4 of Tutorial 8.

(iv) Suppose that $\lambda_i \in \mathbb{Q}$ satisfy $\sum_{i=0}^6 \lambda_i \alpha^i = 0$. Then α is a root of the polynomial $g(x) = \sum_{i=0}^6 \lambda_i x^i \in \mathbb{Q}[x]$. So by Part (i) we have $g(x) = (x^7 - 2)q(x)$ for some $q(x) \in \mathbb{Q}[x]$, and since $\deg g(x) \leq 6$ it follows that $g(x) = 0$. That is, $\lambda_i = 0$ for each i . So the α^i for $1 \leq i \leq 6$ are linearly independent over \mathbb{Q} .

(v) This is a direct application of a theorem from lectures: if an element t in an extension of the field F is algebraic over F with minimal polynomial of degree d then the powers t^i for i from 0 to $d - 1$ form a basis for $F(t)$ considered as a vector space over F . So E is the field $F(t)$.

To see it directly, the first step is to observe that E contains all powers α^n , where $n \geq 0$. Indeed, we can write $n = 7q + r$ with $0 \leq r \leq 6$, and then $\alpha^n = 2^q \alpha^r \in E$. It is now clear that E is closed under multiplication (as well as addition and subtraction) and so is a subring of \mathbb{R} . To check that E is a subfield of \mathbb{R} it remains to check that the inverses of all nonzero elements of E are in E . But any such element has the form $g(\alpha)$ with $g(x) \in \mathbb{Q}[x]$ and $0 \leq \deg g(x) \leq 6$. Since $x^7 - 2$ is irreducible it follows that $\gcd(g(x), x^7 - 2) = 1$, and so there exist $r(x), s(x) \in \mathbb{Q}[x]$ with $r(x)g(x) + s(x)(x^7 - 2) = 1$. Evaluating at $x = \alpha$ shows that $r(\alpha) = g(\alpha)^{-1}$, and $r(\alpha) \in E$ since $r(x) \in \mathbb{Q}[x]$.

(vi) By Part (v), we must find $r(x), s(x) \in \mathbb{Q}[x]$ with $r(x)(x^2 + 1) + s(x)(x^7 - 2) = 1$. This is done by the Euclidean Algorithm. We find $x^7 - 2 = (x^2 + 1)(x^5 - x^3 + x) - x - 2$ and then $x^2 + 1 = (-x - 2)(-x + 2) + 5$. This gives

$$\begin{aligned} 1 &= \frac{1}{5}(x^2 + 1) + \frac{1}{5}(x - 2)(x^7 - 2 - (x^2 + 1)(x^5 - x^3 + x)), \\ &= \frac{1}{5}(x^2 + 1)(1 - (x - 2)(x^5 - x^3 + x)) + \frac{1}{5}(x - 2)(x^7 - 2) \end{aligned}$$

and putting $x = \alpha$ yields $(\alpha^2 + 1)^{-1} = \frac{1}{5}(-\alpha^6 + 2\alpha^5 + \alpha^4 - 2\alpha^3 - \alpha^2 + 2\alpha + 1)$.

3. Noting that $x^2 + 1 \in \mathbb{R}[x]$ is irreducible and that $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}[-i]$ where i and $-i$ are complex roots of $x^2 + 1$, show that there are two different isomorphisms $\mathbb{R}[x]/K \rightarrow \mathbb{C}$, where $K = (x^2 + 1)\mathbb{R}[x]$, one satisfying $f(x) + K \mapsto f(i)$, the other $f(x) + K \mapsto f(-i)$, for all $f(x) \in \mathbb{R}[x]$.

Solution.

Note first that the polynomial $x^2 + 1$ is irreducible over \mathbb{R} . For since its degree is only 2, if it factorized in $\mathbb{R}[x]$ it would have a factor of degree 1, and hence a root in \mathbb{R} , which it does not. As i is a root of $x^2 + 1$ it follows that $x^2 + 1$ is the minimal polynomial of i over \mathbb{R} . (This is because the minimal polynomial of i must be a non-constant monic polynomial in $\mathbb{R}[x]$ and must be a divisor of $x^2 + 1$.) Similarly, $x^2 + 1$

is also the minimal polynomial of $-i$ over \mathbb{R} . Now the evaluation map $\mathbb{R}[x] \rightarrow \mathbb{C}$ given by $f(x) \mapsto f(i)$ (for all $f(x) \in \mathbb{R}[x]$) has kernel $K = (x^2+1)\mathbb{R}[x]$ (since x^2+1 is the minimal polynomial of i over \mathbb{R}) and image $\mathbb{R}[i] = \mathbb{C}$. So the First Isomorphism Theorem yields an isomorphism $\psi: \mathbb{R}[x]/K \rightarrow \mathbb{C}$ such that $f(x) + K \mapsto f(i)$ for all $f(x) \in \mathbb{R}[x]$. Similarly the evaluation map $f(x) \mapsto f(-i)$ from $\mathbb{R}[x]$ to \mathbb{C} also has kernel K and image \mathbb{C} , and gives an isomorphism $\psi': \mathbb{R}[x]/K \rightarrow \mathbb{C}$ such that $f(x) + K \mapsto f(-i)$ for all $f(x) \in \mathbb{R}[x]$. These two isomorphisms are clearly different from each other, as $\psi(x + K) = i$ and $\psi'(x + K) = -i$.

(Note that the inverse of the ψ takes $a + bi \in \mathbb{C}$ to $(a + bx) + K \in \mathbb{R}[x]/K$, for all $a, b \in \mathbb{R}$, while ψ' takes $(a + bx) + K$ to $a - bi$. The composite $\psi'\psi^{-1}$ is an isomorphism $\mathbb{C} \rightarrow \mathbb{C}$ such that $a + bi \mapsto a - bi$ for all $a, b \in \mathbb{R}$. It is also easy to check directly that this is an isomorphism $\mathbb{C} \rightarrow \mathbb{C}$. An isomorphism from a ring to itself is called an *automorphism*.)

4. Let n be a positive integer and $C_n = \{1, g, g^2, \dots, g^{n-1}\}$ the cyclic group of order n . Show that for each positive divisor d of n the set of powers of g^d form a cyclic group of order n/d . Show furthermore that if $\gcd(r, n) = d$ then the set of powers of g^r coincides with the set of powers of g^d .

Solution.

By definition a group is cyclic if it consists of all the powers of some element. It is always true that if G is a group and $x \in G$ then the set of all powers of x forms a subgroup of G . Now if $x^n = x^m$ (where $n, m \in \mathbb{Z}$) then $x^{n-m} = 1$ (the identity element of G). So either the powers of x are in bijective correspondence with integers, via $n \mapsto x^n$, or else there is a least positive integer k such that $x^k = 1$. In this case the elements $1, x, \dots, x^{k-1}$ must be all distinct (since $x^n = x^m$ with $1 \leq n < m \leq k$ would give $x^{n-m} = 1$ with $0 < n - m < k$, contrary to the definition of k); the integer k is called the *order* of x , and equals the number of elements in the cyclic subgroup generated by x .

Turning now to the actual question, we see that the first part is trivial. Since we are given that $g^n = 1$ and $g^r \neq 1$ for $0 < r < n$, it follows that if $n = de$ then $(g^d)^e = g^n = 1$ and $(g^d)^f = g^{df} \neq 1$ for $0 < f < e$ (since $0 < df < n$); thus g^d has order e . Now let $r \in \mathbb{Z}$, and put $d = \gcd(r, n)$. Since $d|r$ we have $r = dc$ for some integer c , and thus $g^r = (g^d)^c$. So g^r is a power of g^d , and hence all powers of g^r are powers of g^d . Conversely, by one of the basic properties of gcd's, there exist integers s and t such that $d = rs + nt$, and hence $g^d = (g^r)^s (g^n)^t = (g^r)^s$, since $g^n = 1$. This shows that g^d , and hence all powers of g^d , are powers of g^r . (We conclude from this exercise that the cyclic subgroups of C_n are in bijective correspondence with the positive divisors of n .)

5. Suppose that $a, b, c \in \mathbb{C}$ are the roots of $x^3 + 9x^2 + 3x - 3 \in \mathbb{Z}[x]$. By expressing the numbers $a^2 + b^2 + c^2$, $a^2b^2 + a^2c^2 + b^2c^2$ and $a^2b^2c^2$ in terms of $a + b + c$, $ab + ac + bc$ and abc , find a polynomial $f(x) \in \mathbb{Z}[x]$ whose roots are a^2 , b^2 and c^2 .

Solution.

We have $x^3 + 9x^2 + 3x - 3 = (x - a)(x - b)(x - c)$. So $a + b + c = -9$, and $ab + ac + bc = 3 = abc$. Observe that $a^2 + b^2 + c^2 = (a + b + c)^2 - 2(ab + ac + bc) = 75$, and $a^2b^2 + a^2c^2 + b^2c^2 = (ab + ac + bc)^2 - 2abc(a + b + c) = 63$. Finally, $a^2b^2c^2 = (abc)^2 = 9$. So $(x - a^2)(x - b^2)(x - c^2) = x^3 - 75x^2 + 63x - 9$.

Since $x^3 + 9x^2 + 3x - 3$ is irreducible over \mathbb{Z} (by Eisenstein with $p = 3$) there is a sense in which the numbers a, b and c are equivalent as far as \mathbb{Z} is concerned. There should not exist any equation over \mathbb{Z} that can distinguish between them. So any equation over \mathbb{Z} that has a^2 as a root should also have b^2 and c^2 as roots. This idea yields another method for finding a suitable $f(x)$; it is the method we used in Question 3 of Tutorial 8.

Since $1, a, a^2$ is a basis for $\mathbb{Q}[a]$ we can express all powers of a as linear combinations of $1, a, a^2$. Specifically, we have that $a^3 = 3 - 3a - 9a^2$, and then multiplying by a gives

$$a^4 = 3a - 3a^2 - 9a^3 = 3a - 3a^2 - 9(3 - 3a - 9a^2) = -27 + 30a + 78a^2,$$

and so on. In fact, for our present purposes we need go no farther: we have

$$a^2 \begin{pmatrix} 1 \\ a \\ a^2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 3 & -3 & -9 \\ -27 & 30 & 78 \end{pmatrix} \begin{pmatrix} 1 \\ a \\ a^2 \end{pmatrix}$$

whence a^2 is a root of the characteristic polynomial of the 3×3 matrix appearing on the right hand side. Exactly the same reasoning says that b^2 and c^2 are roots of the same polynomial. Now

$$\begin{aligned} \det \begin{pmatrix} x & 0 & -1 \\ -3 & x+3 & 9 \\ 27 & -30 & x-78 \end{pmatrix} &= x \det \begin{pmatrix} x+3 & 9 \\ -30 & x-78 \end{pmatrix} - \det \begin{pmatrix} -3 & x+3 \\ 27 & -30 \end{pmatrix} \\ &= x(x^2 - 75x - 234 + 270) - (90 - 27(x+3)) \\ &= x^3 - 75x^2 + 63x - 9. \end{aligned}$$