

Algebra Final: Solutions

Math 123 – Harvard University – Spring 2002

1. Is every ideal in $\mathbb{Q}[x, y]$ generated by (at most) two elements? Justify your answer.

Answer. No: the ideal $I = (xy, x^2, y^2)$ requires at least 3 generators. To see this, let $J \subset I$ be the ideal generated by monomials of degree 3 in (x, y) . Then I/J is a 3-dimensional vector space. Since we have $I^2 \subset J$, this shows I requires at least 3 generators.

2. Give an example of a prime number $p \in \mathbb{Z}$ such that (p) is a prime ideal in the ring $\mathbb{Z}[2^{1/3}] \subset \mathbb{R}$. Justify your answer.

Answer. The ring $\mathbb{Z}[2^{1/3}]/(p)$ is isomorphic to $\mathbb{F}_p[x]/(x^3 - 2)$, so we just need to exhibit a prime p such that $x^3 - 2$ has no roots in \mathbb{F}_p . For example, $p = 7$, works since the cubes in \mathbb{F}_7 are $(0, 1, 6)$.

3. Consider the ideal $I = (5, \sqrt{-10}) \subset R = \mathbb{Z}[\sqrt{-10}]$.

(a) Is I prime? Principal? Justify your answer.

(b) Find a presentation matrix for I as an R -module.

Answer. (a) Since $N(I) = |R/I| = 5$ is prime, I is prime. The norm of the principal ideal $(a + b\sqrt{-10})$ is $a^2 + 10b^2$, which cannot represent 5, so I is not principal.

(b) We have a surjective map $\phi : R^2 \rightarrow I$ given by $\phi(x, y) = 5x + \sqrt{-10}y$. Let $K = \text{Ker } \phi$; it consists of pairs $(x, y) \in R^2$ such that $5x = \sqrt{-10}y$. Thus projection to the x -coordinate sends K isomorphically to the ideal $J \subset R$ given by

$$J = \{x : \sqrt{-10}x \in 2R\}.$$

It is straightforward to check that $J = (2, \sqrt{-10})$. Thus J is the image of the map $R^2 \rightarrow J$ given by $(u, v) \mapsto (2u + \sqrt{-10}v)$. It follows that K is the image of the map $A : R^2 \rightarrow R^2$ given by

$$(u, v) \mapsto u(2, \sqrt{-10}) + v(\sqrt{-10}, -5) = \begin{pmatrix} 2 & \sqrt{-10} \\ \sqrt{-10} & -5 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}.$$

Thus $I = \text{Coker}(A)$, so the matrix above gives a presentation of I .

4. Let $D(f) = \deg(K/F)$ denote the degree of the splitting field K of a monic polynomial f in $F[x]$, where F is a field of characteristic zero.

(a) Show that if $f(x) = g(x)h(x)$, then $D(f)$ divides $D(g)D(h)$.

(b) Give an example where $D(f) = D(g)D(h) > 3$.

(c) Give an example where g and h have different splitting fields, and yet

$$\max(D(g), D(h)) < D(f) < D(g)D(h).$$

Answer.

(a) The splitting field K_f of f contains the splitting fields K_g, K_h of g and h . Since K_g and K_h are Galois over F , they are invariant under $\text{Gal}(K_f/F)$. By restricting an automorphism to each of these subfields, we obtain a group homomorphism

$$\phi : \text{Gal}(K_f/F) \rightarrow \text{Gal}(K_g/F) \times \text{Gal}(K_h/F).$$

Since the roots of g and h generate K_f , any automorphism fixing both K_g and K_h is the identity. Thus ϕ is injective, so it defines a subgroup of the product on the right. Therefore $D(f) = |\text{Gal}(K_f/F)|$ divides $D(g)D(h)$.

(b) $f(x) = (x^2 - 2)(x^2 + 1)$. Here $D(g) = D(h) = 2$, $D(f) = 4$.

(c) $f(x) = (x^4 - 2)(x^4 - 3)$ works. Here $D(g) = D(h) = 8$ and $D(f) = 32$. The splitting field of f is $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{3}, i)$.

5. Prove that any automorphism ϕ of $K = \mathbb{C}(x)$ over $F = \mathbb{C}$ satisfies $\phi(x) = (ax + b)/(cx + d)$ for some $a, b, c, d \in \mathbb{C}$, $ad - bc \neq 0$.

Proof. Every rational function $f \in \mathbb{C}(x)$ can be written in the form $f(x) = p(x)/q(x)$ where p and q are polynomials with no common roots. Define $\deg(f) = \max(\deg(p), \deg(q))$. It is not hard to check that

$$\deg(f(g(x))) = \deg(f) \cdot \deg(g).$$

Now let $f = \phi(x) \in \mathbb{C}(x)$. Then $\mathbb{C}(x) = \mathbb{C}(f)$. Consequently, $x = g(f(x))$ for some rational function g . Since $\deg(x) = 1 = \deg(g) \cdot \deg(f)$, we have $\deg(f) = 1$, which gives the result above. ■

Mark each assertion True (T) or False (F).

1. **False.** There exists a prime ideal I in a ring R such that $|R/I| = 143$.
(The quotient R/I is a finite field, so its order must be a power of a prime.)
2. **False.** If every pair of nonzero elements f, g in a ring R have a greatest common divisor (well-defined up to units), then R is a PID.
(E.g. R might be $\mathbb{Z}[x]$, a UFD which is not a PID.)
3. **True.** There exists a nonzero polynomial $\phi(u, v) \in \mathbb{Z}[u, v]$ such that $\phi(x^2 + x + 1, x^{11} + x^5 - 1) = 0$.
(Let F be the subfield of $K = \mathbb{Q}(x)$ generated by $x^2 + x + 1$. Then K/F has degree two, so any polynomial in x is algebraic over F .)
4. **True.** The ring $\mathbb{Z}[x, y]/(y^2 + x^3 + 1)$ is a finitely-generated $\mathbb{Z}[x]$ -module.
5. **False.** Let $f(x) \in \mathbb{Q}[x]$ be the irreducible polynomial of $\alpha \in \mathbb{R}$. If $\deg(f)$ is a power of two, then α is a constructible number.
(This would imply, for example, that polynomials of degree 8 are solvable by radicals.)
6. **False.** If the extensions K/E and E/F are solvable, then K/F is also solvable.
(One can make examples where K/F is not even be Galois, e.g. $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}(\sqrt[4]{2})$.)
7. **False.** The Galois group of the splitting field of $x^n - 1$ over \mathbb{Q} is cyclic for any $n \geq 1$.
(The Galois group is $(\mathbb{Z}/n)^*$, which is not always cyclic; e.g. $(\mathbb{Z}/15)^*$ has 4 elements of order 2, namely $(1, 4, 11, 14)$, so it is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/4$.)
8. **True.** The polynomial $f(x) = x^{12} + 7x^8 + 1$ is solvable by radicals.
9. **False.** The ring of algebraic numbers in \mathbb{C} is a finitely-generated module over the ring of algebraic integers.
(Let $A = (a_i/b_i)_1^n$ be a finite list of algebraic numbers, written as quotients of algebraic integers. The module generated by A over the algebraic integers includes only numbers with denominators no large than $b_1 \cdots b_n$.)
10. **False.** If K/F is a Galois extension and $[K : F] = p$, p prime, then K is the splitting field of a polynomial of the form $f(x) = x^p - a$.