

1:

(a) This is the fourth isomorphism theorem for rings which can be proven as follows: by the fourth isomorphism theorem for groups, we have that there is a bijective correspondence

$$\{\text{additive subgroups of } R \text{ containing } I\} \rightarrow \{\text{additive subgroups of } R/I\}$$

Now let J be an additive subgroup of R containing I .

We first show that J is a ring in R if and only if J/I is a ring in R/I .

Let $a, b \in J$. Then we have $\pi(a)\pi(b) = \pi(ab)$ and this is in J/I if and only if $ab \in J$.

We have our correspondence if we can show that J is an ideal if and only if J/I is an ideal.

Let $r \in R$ and $j \in J$. In R/I we have $\pi(r)\pi(j) = \pi(rj)$ and $\pi(j)\pi(r) = \pi(jr)$, and this is in J/I if and only if rj and jr are in J . Thus J is an ideal containing I if and only if J/I is an ideal.

(b) The correspondence in (a) was given by the canonical homomorphism π .

Now let J be a radical ideal in R containing I . Assume $\pi(r^k) = \pi(r)^k \in \pi(J)$. Then $r^k \in \pi^{-1}(\pi(J)) = J$, so $r \in J$ as it is radical, and thus $\pi(r) \in \pi(J)$, so $\pi(J)$ is radical.

Similarly, for any radical ideal $\pi(J)$ in R/I , we have that if $r^k \in J$ then $\pi(r)^k = \pi(r^k) \in \pi(J)$ so $\pi(r) \in \pi(J)$ as it is a radical ideal, and thus $r \in \pi^{-1}(\pi(J)) = J$, so J is a radical ideal.

We thus find that the bijective correspondence induces a bijection between radical ideal in R containing I , and radical ideals in R/I .

(c) Let $M \subset R$ be a maximal ideal containing I . Assume that there exists an ideal $\pi(S)$ in R/I such that $\pi(M) \subset \pi(S) \subset R/I$ - where S is an ideal in R containing I which we can assume by (a). Then applying π^{-1} , we have $M \subset S \subset R$. Therefore $S = M$ or $S = R$, so $\pi(S) = \pi(M)$ or $\pi(S) = R/I$. So $\pi(M)$ is a maximal ideal.

Conversely, let $\pi(M)$ be a maximal ideal in R/I with $I \subset M$ and M ideal. Assume there exists an ideal S in R containing I such that $M \subset S \subset R$. Then $\pi(M) \subset \pi(S) \subset R/I$, and $\pi(S)$ is an ideal, so it must either be $\pi(M)$ or R/I . By A we then get S is M or R , so M is a maximal ideal.

Thus the bijection in (a) induces a bijection between maximal ideals in R containing I and maximal ideals in R/I .

2.

(a) We assume $I \neq (1) = k[x_1, \dots, x_n]$ - i.e. I is proper.

According to a lemma from lecture notes 4, we have that I is contained in a maximal ideal - so the below intersection over maximal ideals containing I is nonempty.

Assume $I \subset k[x_1, \dots, x_n]$ is a radical ideal with k algebraically closed. Then

$$I \subset \bigcap_{I \subset A, A \text{ max ideal}} A = \mathcal{A}$$

Let $f \in \bigcap_{I \subset A, A \text{ max ideal}} A$.

Since k is algebraically closed, we get by weak Nullstellensatz 2 that all the maximal ideals A containing I are of the form $(x_1 - a_1, \dots, x_n - a_n) = I(a_1, \dots, a_n)$. Let now $\alpha \in V(I)$ and assume $\alpha \notin V(f)$. Write $\alpha = (\alpha_1, \dots, \alpha_n)$. Then $I \subset (x_1 - \alpha_1, \dots, x_n - \alpha_n)$ which is a maximal set, hence $f \in \bigcap_{I \subset A, A \text{ max ideal}} A \implies f \in (x_1 - \alpha_1, \dots, x_n - \alpha_n)$ but then $\alpha \in V(f)$, contradiction. Thus $V(I) \subset \bigcap_{f \in \mathcal{A}} V(f) = V\left(\bigcup_{f \in \mathcal{A}} (f)\right) = V(\mathcal{A})$ so

$$\mathcal{A} \subset \sqrt{\mathcal{A}} = I(V(\mathcal{A})) \subset I(V(I)) = I$$

Thus $I = \mathcal{A}$.

(b)

We find $V(I)$: if $y^3 - y = 0$ we have $y = 0$ or $y = \pm 1$. If $y = 0$ then $x^2 - 2xy^4 + y^6 = x^2 = 0$ if and only if $x = 0$.

If $y = \pm 1$, then $x^2 - 2xy^4 + y^6 = x^2 - 2x + 1 = (x - 1)^2 = 0$ if and only if $x = 1$.

Thus $V(I) = \{(0, 0), (1, 1), (-1, 1)\}$ and so $\sqrt{I} = I(V(I)) = I(\{(0, 0), (1, 1), (-1, 1)\}) = I((0, 0)) \cap I((1, 1)) \cap I((-1, 1)) = (x, y) \cap (x - 1, y - 1) \cap (x + 1, y - 1)$. Each of these is a maximal ideal by weak Nullstellensatz 2 as they are one point sets and \mathbb{C} is algebraically closed - or alternatively as they are the kernels of the evaluation maps.

3: Assume $x^2 - yz = 0$ and $xz - x = 0$. Then $x = 0$ or $z = 1$.

If $x = 0$, we have $yz = 0$ which implies $y = 0$ or $z = 0$ as \mathbb{C} is an integral domain.

If $z = 1$ we get $x^2 = y$.

Conversely, each of these solution sets satisfies the system. Thus we find

$$V(x^2 - yz, xz - x) = V(y) \cup V(z) \cup V(x^2 - y)$$

Now $I(V(y)) = \sqrt{(y)} = (y)$ which is a prime ideal since

$$k[x, y, z]/(y) \cong k[x, z]$$

which is an integral domain and hence y is a prime ideal and thus also $\sqrt{(y)} = (y)$. Interchanging the roles of y and z , we find that (z) is also a prime ideal. It follows from proposition 1 in section 5 that $V(y), V(z)$ are irreducible.

Now, let $\varphi: k[x, y, z] \rightarrow k[x, z]$ be the map sending $y \rightarrow x^2$. It has kernel $(x^2 - y)$, and is trivially surjective as any $f \in k[x, z]$ is of the form $\sum_{i,j} c_{i,j} x^i z^j$ and $\varphi\left(\sum_{i,j} c_{i,j} x^i z^j\right) = \sum_{i,j} c_{i,j} x^i z^j$. Thus

$$k[x, y, z]/(x^2 - y) \cong k[x, z]$$

which is an integral domain and thus $(x^2 - y)$ is prime. Therefore $\sqrt{(x^2 - y)} = (x^2 - y)$ and $V(x^2 - y)$ is irreducible by proposition 1 section 5 since $I(V(x^2 - y)) = \sqrt{(x^2 - y)} = (x^2 - y)$ is prime.

4:

(a) Let \mathcal{A} be the set of elements in L that are algebraic over k . Since for any $\alpha \in k$, α is the root of $x - \alpha \in k[x]$, we have $k \subset \mathcal{A}$ and thus also $0, 1 \in \mathcal{A}$.

If $\alpha, \beta \in \mathcal{A}$, then there exist $f, g \in k[x]$ such that $f(\alpha) = 0 = g(\beta)$.

By the corollary in section 9, we have that the elements of L that are algebraic over k form a subring of L containing k . To show that this subring is, in fact, a subfield, we must show that for any α algebraic over k , α^{-1} is also algebraic over k .

We use the hint: suppose $v \neq 0$ is algebraic over k . Then there exists $f \in k[x]$, say $f(x) = \sum_{i=1}^n a_i x^i$, such that $f(v) = 0$ - we can assume that $a_n = 1$ as $a_n \in k$ so we can divide out by a_n^{-1} since k is a field. Thus assume f is monic.

In particular, this means that $v^n + a_{n-1}v^{n-1} + \dots + a_1v + a_0 = 0$. If $a_0 = 0$, then $v(v^{n-1} + \dots + a_1) = 0$, so since v is not a zero divisor in L , we have $v^{n-1} + \dots + a_1 = 0$. Thus we have reduced the degree once. We can continue this if $a_1 = 0$ until we get some $a_i \neq 0, i > 1$ - this must eventually occur as after at $n - 1$ steps, we would get $v + a_{n-1} = 0$ and thus $a_{n-1} \neq 0$ as $v \neq 0$. Assume thus without loss of generality that $a_n \neq 0$. Then $v(v^{n-1} + \dots + a_1) = -a_n$. Then dividing through by $v^{n-1}(-a_n)^{-1}$ we get

$$(-a_n)^{-1} + \dots + (-a_n)^{-1}a_1v^{n-1} + v^{-n} = 0$$

so v^{-1} is the root of a monic polynomial in $k[x]$ and thus algebraic over k .

(b) We must show that any nonzero element of R has an inverse. Let $r \in R$ be nonzero. Since L is a finite extension of k it is also an algebraic extension by the claim in lecture notes 5. Hence there exists a monic polynomial $f \in k[x]$ such that $f(\frac{1}{r}) = 0$. Let $f(x) = \sum_{i \leq n} a_i x^i$, so $0 = f(\frac{1}{r}) = \sum_{i \leq n} a_i r^{-i}$. Multiplying by r^{n-1} , we get $\frac{1}{r} = -\frac{1}{a_n} \sum_{i \leq n-1} a_i r^{n-1-i} \in R$. Hence each $r \in R$ has an inverse, so R is a field.

5: If $\alpha \in L'$ is algebraic over L , then there exist $c_i \in L$ such that

$a^n = c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}$. Let $S = k[c_0, c_1, \dots, c_{n-1}, \alpha] = \left\{ \sum a_{(i)} c_0^{i_0} \dots c_{n-1}^{i_{n-1}} \alpha^{i_n} \right\}$. Define the homomorphism $\varphi: k[x_0, \dots, x_{n-1}, x_n] \rightarrow S$ by sending $x_i \rightarrow c_i$ and $x_n \rightarrow \alpha$. Then S a subfield of L' that is k ring-finite. By Zariski, S is module-finite and hence algebraic over k . Thus there exists $f \in k[x]$

such that $f(\alpha) = 0$

Alternative, we can show it by repeated uses of proposition 3, section 9:

since c_0, \dots, c_n are in L , they are algebraic, so $S' = k[c_0, \dots, c_n]$ is module finite by repeated applications of proposition 3 with problem 1.45.(a) - transitivity of module-finiteness.

Then $S = S'[\alpha]$ is module finite over S' by the first part of the problem. Since $k[\alpha] \subset S$, we have that $k[\alpha]$ is finite and thus α is algebraic over k .