1. Let q be a prime, $R = \mathbb{Z}$ and $S = \mathbb{Z}[\sqrt{q}]$. Find the primes in S lying over each prime $p \in \mathbb{Z}$ (use quadratic reciprocity).

Solution. Let $\mathfrak{p}$ be a prime ideal in S lying over (p). This means that $\mathfrak{p}$ contains p, so $S/\mathfrak{p}$ is a quotient of $\mathbb{F}_p[z]/(z^2-q)$. If $p = q$ then we must have $S/\mathfrak{p} = \mathbb{F}_p$, so $\mathfrak{p} = (\sqrt{p})$. Otherwise, $\mathbb{F}_p[z]/(z^2-q)$ is $\mathbb{F}_{p^2}$ if q is a nonsquare mod p, in which case $\mathfrak{p} = (p)$, and $\mathbb{F}_p[z]/(z^2-q) = \mathbb{F}_p \times \mathbb{F}_p$ if q is a square mod p, in which case we have two choices for $\mathfrak{p}$. To tell if q is a square, recall quadratic reciprocity. Namely, 2 is a square mod $p > 2$ iff p is ± 1 mod 8, and $q > 2$ is a square mod p iff p IS NOT a square mod q when p, q are both of the form $4k+3$, and iff p IS a square mod q otherwise.

2. Let $R = \mathbb{C}[x, y, z]/(x^2 + y^2 - z^2 + 1)$. For a nonzero $v \in \mathbb{C}^3$, let $E_v \subset (\mathbb{C}^3)^*$ be the space of linear functions a such $a(v) = 0$, and let a_1, a_2 be a basis of E_v. Find all v for which R is module finite over $\mathbb{C}[a_1, a_2]$ (i.e., we have an instance of Noether normalization).

Solution. Consider the inner product $(x, y, z)^2 = x^2 + y^2 - z^2$. If $v^2 \neq 0$ then after renormalizing v we can find a basis e_1, e_2, $v = e_3$ such that $e_ie_j = 0$ for $i \neq j$ and $e_1^2 = 1$, $e_2^2 = 1$, $e_3^2 = 1$. So if x_1, x_2, x_3 are the coordinates with respect to this basis, then the ideal is generated by $x_1^2 + x_2^2 + x_3^2 - 1$. So $R = \mathbb{C}[x_1, x_2, x_3]/(x_1^2 + x_2^2 + x_3^2 - 1)$ and this is clearly module finite (free of rank 2) over $\mathbb{C}[x_1, x_2]$.

However, suppose that $v^2 = 0$. In this case we can find a basis e_1, e_2, $v = e_3$ such that $e_1^2 = 1$, $e_2e_3 = e_3e_2 = 1$, and other inner products are zero. So if x_1, x_2, x_3 are the coordinates with respect to this basis, then the ideal is generated by $x_1^2 + x_2x_3 - 1$. So $R = \mathbb{C}[x_1, x_2, x_3]/(x_1^2 + x_2x_3 - 1)$. To check if this is module finite over $\mathbb{C}[x_1, x_2]$, let us mod out by x_1. We get $\mathbb{C}[x_2, x_3]/(x_2x_3 - 1) = \mathbb{C}[x_2, x_2^{-1}]$, which is not module finite over $\mathbb{C}[x_2]$. So R is not module finite over $\mathbb{C}[x_1, x_2]$.

3. (a) Let I be the ideal of polynomials in $\mathbb{C}[x, y, z]$ which vanish on the three coordinate axes. Find a finite set of generators for I.

(b) Let J be the ideal of polynomials in x, y, z that vanish on the plane $z = 0$ and on the z-axis. Find a finite set of generators for J.

(c) Let $R = \mathbb{C}[x, y, z]/J$. Find the Krull dimension of R.

(d) Let S be a ring of Krull dimension d, and $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset ... \subset \mathfrak{p}_r$ be a strictly increasing chain of primes in S which cannot be refined (i.e., we cannot insert more primes into it). Does it follow that $r = d$?

Solution. (a) I is generated by xy, xz, yz.

(b) J is generated by xz and yz.

(c) The Krull dimension of R is 2.

(d) No. Let $S = \mathbb{C}[x] \oplus \mathbb{C}$. Then $d = 1$, but $\mathbb{C}[x] \subset S$ is both a maximal and minimal prime, so cannot be extended to a chain, so $r = 0$. Another counterexample is the ring from (c).

4. Let I be the ideal in $\mathbb{C}[x, y]$ generated by xy^2 and x^2y. Construct infinitely many irredundant primary decompositions of I.

Solution. One can take $Q_1 = (x)$, $Q_2 = (y)$, and $Q_3 = (x^n, x^2y, xy^2, y^m)$.

5. Let p be a prime. Show that there are exactly four isomorphism classes of Artinian rings with p^2 elements, and describe these rings. Which of them are algebras over the field $\mathbb{F}_p$?

Solution. Any such ring A is a direct sum of local ones, and we can have 1 or 2 summands. For 2 summands, it has to be $\mathbb{F}_p \oplus \mathbb{F}_p$. So it remains to consider the local case. If A is a field, $A = \mathbb{F}_{p^2}$. Otherwise, A has a maximal ideal I such that $A/I = \mathbb{F}_p$, and I is 1-dimensional. If $p = 0$ in A, then we have $\mathbb{F}_p \subset A$, and choosing any $x \in I$, $x \in 0$, we get $A = \mathbb{F}_p[x]/x^2$. If $p \neq 0$ in A, then $p \in I$, so $p^2 = 0$, and $A = \mathbb{Z}/p^2\mathbb{Z}$. This is the only one which is not an $\mathbb{F}_p$-algebra.