1. (a) They are all integral: it suffices to show that x, y, z are, since K is contained in the subring and the integral elements form a ring. This follows because x, y, z satisfy the respective monic polynomials $U^{13} + U^5 - (x^{13} + x^5) = 0$, $V^{17} + V^7 - (y^{17} + y^7) = 0$, and $W^{23} + W^{11} - (z^{23} + z^{11}) = 0$ with coefficients in $K[x^{13} + x^5,\, y^{17} + y^7,\, z^{23} + z^{11}]$. (There is no need to use a different letter for the variable in each of the three equations, but I thought it might keep things clearer.)

(b) We show $s = \dfrac{1 + \sqrt{-19}}{2}$ has the required property. s satisfies the monic equation $(*)\quad s^2 - s + 5 = 0$, and so is integral over $\mathbb{Z}$. Moreover, $\mathbb{Z}[s] = \mathbb{Z} + \mathbb{Z}s$ (when we multiply two elements, we can use the equation $(*)$ to get rid of the s^2 term). Suppose $t = a + b\sqrt{-19}$ is integral over $\mathbb{Z}$, where $a, b \in \mathbb{Q}$. Since $\mathbb{Z}$ is normal, this implies that if $b = 0$, then $a \in \mathbb{Z}$, and that if $b \neq 0$ then the minimal monic polynomial f of t has coefficients in $\mathbb{Z}$, and this is the quadratic polynomial whose other root is $a - b\sqrt{-19}$. Then $f(x)$ is $x^2 - 2ax + a^2 + 19b^2$, and $2a \in \mathbb{Z}$. The we can subtract sn, where $n \in \mathbb{Z}$, from t to get a new choice of t for which $a = 0$. Hence, we may assume that $t = b\sqrt{-19}$. It will then suffice to show that $b \in \mathbb{Q}$ is an integer. Write $b = m/n$ in lowest terms. Then $(b\sqrt{-19})^2 = m^2(-19)/n^2$ is integral over $\mathbb{Z}$, and since it $\in \mathbb{Q}$ it must in $\mathbb{Z}$. If there is an prime that divides n, it does not occur in m^2, and it will occur to an even power in n^2 and cannot be cancelled by 19. It follows that $n = \pm 1$, and $b = m/n = \pm m$ is an integer.

2. Following the suggestion, the roots of $h = fg$, the product, all satisfy the monic polynomial $h(x) = 0$. All the coefficients of h are in R. Hence, all roots of h are integral over R. These include all of the roots of f and of g, which are therefore integral over R. The coefficients of f are, up to sign, the elementary symmetric functions of the roots of f, and so they are integral over R. The same holds for the coefficients of g.

3. We want to choose the matrix so that x_n^d occurs with nonzero coefficient in F_d. This is equivalent to getting a nonzero result when one substitutes 0 for all the x_i such that $1 \leq i \leq n-1$. After applying the matrix, we substitute $a_{i1}x_1 + \cdots + a_{in}x_n$ for x_i, and after substituting zeros for the x_i other than x_n, we get $a_{in}x_n$. Therefore, we simply need that $F_d(a_{1n}x_n, a_{2n}x_n, \ldots, a_{nn}x_n) \neq 0$, and since F_d is homogeneous of degree d, this is $F_d(a_{1n}, a_{2n}, \ldots, a_{nn})x_n^d$. Since a polynomial with a nonzero coefficient does not vanish identically over an infinite field,[1] we can choose $v = (a_{1n}, a_{2n}, \ldots, a_{nn})$ so that F_d does not vanish as this point, and the a_{in} cannot all be 0. This gives the nth row of the required matrix. We can extend $v \neq 0$ to a basis for K^n, and use the rest of the basis vectors for the other rows of the matrix to obtain the required invertible matrix.

4. (a) By Hilbert's Nullstellensatz, if there were no solution over K, the polynomials would generate the unit ideal in $K[x_1, \ldots, x_n]$. But then this would remain true over the larger field L, which shows that they have no solution in L, a contradiction. $\square$

(b) Suppose $f = gh$ over S, where f has degree d, g has degree a, h has degree b, with $a, b < d$ (one will have $a + b = d$). Introduce one variable y_μ for every monomial μ of degree

[1] This follows by induction on the number n of variables. If $n = 1$, the number of roots is bounded by the degree. At the inductive step, think in $D[x_n]$, where $D = K[x_1, \ldots, x_{n-1}]$. Some coefficient in D is not 0. By the induction hypothesis, we may substitute elements of K for $x_1, \ldots, x_{n-1}$ to get a polynomial in $K[x_n]$ with a nonzero coefficient, and we have reduced to the case $n = 1$.

a in $x_1, \ldots, x_n$, and one variable z_ν for every monomial ν of degree b in $x_1, \ldots, x_n$. From the equation $f = (\sum_\mu y_\mu \mu)(\sum_\nu z_\nu \nu)$, one obtains a system of equations by equating each coefficient of a monomial in $x_1, \ldots, x_n$ on the left (these are the coefficients of f) to the corresponding coefficient (a polynomial over the image of $\mathbb{Z}$ in the y_μ and z_ν) occurring on the right. The problem of factoring f into the product of a polynomial in of degree a times a polynomial of degree b in R (respectively, in S) is equivalent to finding a solution of these equations such that the values of y_μ, z_ν are in K (respectively, in L). Since there is a solution in L, part (a) of this problem tells us that there is a solution in K. $\square$

5. The Krull dimension is the transcendence degree over K, and it will suffice to show that monomials of the form $\underline{x}^{\underline{b}} = x_1^{b_1} \cdots x_n^{b_n}$ are algebraically independent over K iff their exponent vectors $\underline{b}$ are linearly independent over $\mathbb{Q}$. Suppose one has a relation $q_1\underline{b}_1 + \cdots + q_k\underline{b}_k = 0$ with the $q_i \in \mathbb{Q} - \{0\}$. Clear denominators to get a relation where the $q_i \in \mathbb{Z}$. But then $(\underline{x}^{b_1})^{q_1} \cdots (\underline{x}^{\underline{b}_k})^{q_k} = 1$ gives a corresponding algebraic relation on the corresponding monomials $\underline{x}^{\underline{b}_i}$ (Some q_i may be < 0). Hence, it suffices to show that if $\underline{b}_1, \ldots, \underline{b}_k$ are linearly independent over $\mathbb{Q}$, then the monomials $\underline{x}^{\underline{b}_i}$ are algebraically independent over K. If not there is an algebraic relation on them: they will satisfy a polynomial $\sum_{\underline{j}} c_{\underline{j}} \underline{Z}^{\underline{j}} = 0$, where $\underline{Z}$ denotes variables $Z_1, \ldots, Z_k$, $\underline{j}$ runs through a family of distinct elements of $\mathbb{N}^k$, and the $c_{\underline{j}} \in K - \{0\}$. The terms cannot cancel unless for distinct values of the κ-tuple $\underline{j}$, two of the terms $\underline{Z}^{\underline{j}}$ become equal when we substitute the values $\underline{x}^{\underline{b}_i}$ for the Z_i: otherwise, all the terms are nonzero scalar multiples of distinct monomials in the variables $\underline{x}$, and there can be no cancellation. If this happens for $\underline{j}$ and $\underline{j}'$ we have $(\underline{x}^{\underline{b}_1})^{j_1} \cdots (\underline{x}^{\underline{b}_k})^{j_k} = (\underline{x}^{\underline{b}_1})^{j_1'} \cdots (\underline{x}^{\underline{b}_k})^{j_k'}$, and this implies $\sum_{t=1}^{k}(j_t - j_t')\underline{b}_t = 0$, while not all the $j_t - j_t'$ vanish, a contradiction. $\square$

6. Every element of $V - \{0\}$ has the form at^n, where a is a unit of V and $n \in \mathbb{N}$, and so every element of $L - \{0\}$ has the form at^n, where a is a unit of V and $n \in \mathbb{Z}$. Thus elements of $E - \{0\}$ have the form au_n, where a is a unit of V and $n \geq 1$. Clearly, every submodule $M \neq 0$ of E is determined by which of the u_n it contains, and these form an initial segment or all of the positive integers: if $u_n \in E$, so is u_h for $1 \leq h \leq n$, since $u_h = t^{n-h}u_n$. Hence, $M \subseteq E$ is 0, or contains finitely many u_i, in which case it is Vu_n for the largest n such that $u_n \in M$ or else $M = E$. Any strictly descending chain, after the first term, which might be E, has second term of the form 0 or Vu_n. The first case is clear. If the second term is Vu_n, the longest strictly descending chain from that point is $Vu_n \supset Vu_{n-1} \supset \cdots \supset Vu_1 \supset 0$. Hence, E has DCC. However $0 \subset Vu_1 \subset \cdots \subset Vu_n \subset \cdots$ is an infinite strictly ascending chain, so E does not have ACC.

EC3 Let f be in the fraction field of R, which is the same as the fraction field of R_a and of R_b, and integral over R. Then $f \in R_a$ and $f \in R_b$, since those rings are normal, and it suffices to show that $R_a \cap R_b = R$. Suppose that $r/a^m = s/b^n$, where $r, s \in R$. Then $sa^m = rb^n$. If we knew that $(*)$ $\quad a^mR \cap b^nR = a^mb^nR$, we could then conclude that $sa^m = rb^n = ta^mb^n$ with $t \in R$. It follows that $s = tb^n$,and so $s/b^n = t \in R$, as required. It remains to prove $(*)$. We use induction on m to show that $a^mR \cap bR = a^mbR$. It then follows by essentially the same induction (with a^m in the role of b and b in the role of a) that $a^mR \cap b^nR = a^mb^nR$.

The case $m = 1$ for $(*)$ is given. Assume the result when $m > 1$ is replaced by $m-1$. Then if $u = a^mr \in a^mR \cap bR \subseteq abR$ we know that $u = abv$ with $v \in R$, and so $u = a^mr = abv$.

Then $u' = a^{m-1}r = bv$, where $u = au'$. By the induction hypothesis, u' can be written $a^{m-1}bw$. But then $r = bw$, and $u = au' = a(a^{m-1}bw) = a^m bw$, as required. $\square$
[Alternate: check that the statement $aR \cap bR = abR$ is equivalent to the statement that the image of a is not a zerodivisor in R/bR. This implies that the image of a^m is not a zerodivisor in R/bR, and, working backward from this, that $a^m \cap bR = a^m bR$. $\square$]

EC4. By the Noether normalization theorem, R is module-finite over $A = K[x]$, the polynomial ring in one variable: suppose that R has n generators as an A-module. We show that every ideal I in R needs at most n generators as an A-module, and, hence, as an R-module. We can map $A^{\oplus n}$ onto R and consider the inverse M image of the ideal I in $A^{\oplus n}$. It suffices to show that $M \subseteq A^{\oplus n}$ needs at most n generators over A. By the theory of modules over a PID, M is A-free of rank at most n, and so needs at most n generators as an A-module. $\square$