Solutions 1

Each question part is worth 1 point.

1. Let $R \subseteq S \subseteq T$ be commutative rings and let M be an S-module.
(a) (4.1 of Eisenbud) Show that if S is finite over R and M is finitely generated as an S-module, then M is finitely generated as an R-module.
(b) Suppose that S is integral over R and T is integral over S. Show that T is integral over R.

Solution. (a) If S is generated as an R-module by elements $s_1, \ldots, s_c$ and M is generated as an S-module by elements $m_1, \ldots, m_d$ then we claim that M is generated as an R-module by the elements $s_i m_j$. Every element of M can be written $m = \sum_j a_j m_j$ for certain elements $a_j \in S$. We may also write each $a_j = \sum_i b_{ij} s_i$ with $b_{ij} \in R$. Putting this together, $m = \sum_j (\sum_i b_{ij} s_i) m_j = \sum_{i,j} b_{ij} s_i m_j$. Thus M is finitely generated as an R-module.
(b) Each element a in T is the root of a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in S$. The subring S' of S generated by $a_0, \ldots, a_{n-1}$ is finite over R by integrality and a lemma in class. Also the subring $S'[a]$ is finitely generated as an S'-module because the monic polynomial of which a is a root has coefficients in S', so a is also integral over S'. Thus by part (a), $S'(a)$ is finitely generated as an R-module. It follows that a is integral over R by another lemma in class. Hence T is integral over R.

2. (4.2 of Eisenbud with R and S interchanged.) Let k be a field, $R = k[t]$ and suppose $R \subseteq S$ is a containment of rings, where S is supposed to be a domain.
(a) Show that if S is finitely generated as an R-module, then S is free as an R-module.
(b) Show by giving a basis that if $S = k[x,y]/(x^2 - y^3)$ and $t = x^m y^n$, then the rank of S as an R-module is $3m + 2n$.
(c) Assuming again only that the domain S is finitely generated as an R-module, let $\bar{S}$ be the integral closure of S in its field of fractions. Assume Noether's theorem 4.14 that $\bar{S}$ is again finitely generated (and thus free) as an R-module. Show that it has the same rank as S.
[Feel free to make use of the structure theorem for finitely generated modules over a PID.]

Solution. (a) Because S is a domain, no non-zero element of R annihilates any non-zero element of S, so as an R-module S is torsion-free. Also R is a PID and S is finitely generated as an R-module, so by the structure theorem for such modules S is free.
(b) Because $\bar{x}^2 = \bar{x}^3$ in S, the elements $1, \bar{y}, \bar{y}^2, \ldots, \bar{x}, \bar{x}\bar{y}, \bar{x}\bar{y}^2, \ldots$ form a basis of S as an R-module. Multiplying each basis element by $x^m y^n$ gives another basis element, and so S is the direct sum of cyclic R-modules that have subsets of these basis elements as a basis. Two basis elements $\bar{x}^a \bar{y}^b$ and $\bar{x}^c \bar{y}^d$ lie in the same R-submodule if and only if $(c - a, d - b)$ is a multiple of (m, n) modulo the subgroup of $\mathbb{Z}^2$ generated by $(2, -3)$, if

and only if $(c-a, d-b)$ lie in the same coset of the subgroup of $\mathbb{Z}^2$ generated by the rows of $\begin{pmatrix} 2 & -3 \\ m & n \end{pmatrix}$. By the theory of Smith normal form, this subgroup has index the determinant of the matrix, which is $3m+2n$, so this is the number of such cosets.
(c) Let $K(R)$ be the field of fractions of R, realized as the subfield of $K(S)$ generated by R. The elements of S are algebraic over R, so $K(S)$ is an algebraic extension of $K(R)$. We claim that a basis for S as an R-module is also a basis for $K(S)$ as a $K(R)$-module. This is because a basis of S as an R-module is also independent over $K(R)$ (clear denominators in a relation over $K(R)$ to get a relation over R), and it spans $K(S)$ over $K(R)$ because each element in the span, being algebraic, has its inverse in the span of its powers, which lie in the $K(R)$-span of S. We also have that $K(S) = K(\bar{S})$, and again because $\bar{S}$ is finitely generated as an R-module, a basis of $\bar{S}$ over R is also a basis of $K(S)$ over $K(R)$. Such bases have the same size, so the ranks of S and $\bar{S}$ are the same.

3. (4.7 of Eisenbud) Show that the Jacobson radical of R is

$$J = \{r \in R \mid 1 + rs \text{ is a unit for every } s \in R\}.$$

Solution. Let $L = \{r \in R \mid 1 + rs \text{ is a unit for every } s \in R\}$. If $r \in J$ and $1 + rs$ is not a unit for some s then $1 + rs$ generates a proper ideal of R, so $1 + rs \in \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Thus $1 \in \mathfrak{m}$, a contradiction, because r lies in every maximal ideal. Thus $J \subseteq L$. On the other hand, if $r \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ then $Rr + \mathfrak{m} = R$, so that $1 = -rs + \mathfrak{m}$ for some $s \in R$. This means that $1 + rs \in \mathfrak{m}$ is not a unit, and shows that $L \subseteq J$.

4. (4.11 of Eisenbud minus the graded bit)
(a) Use Nakayama's lemma to show that if R is a commutative local ring and M is a finitely generated projective module, then M is free.
[Identify the radical, consider factoring out its action, produce a map from a free module that is an isomorphism with M.]
(b) Use Proposition 2.10 to show that a finitely presented module M is projective if and only if M is locally free, in the sense that the localization M_P is free over R_P for every maximal ideal P of R (and then of course M_P is free over R_P for every prime ideal P of R).

Solution. (a) If R is a local ring it has a unique maximal ideal P, and this is also the radical (the intersection of the maximal ideals). Let M be a finitely generated projective R-module. Now M/PM is a finite dimensional vector space over the field R/P, and if it has dimension d we can take a surjection $F = R^d \to M/PM$. By projectivity of F it lifts to a homomorphism $\phi : F \to M$. This has the property that $\phi(F) + PM = M$ so $\phi(F) = M$, i.e. ϕ is surjective, by Nakayama's lemma. This ϕ is split because M is projective, so there is a homomorphism $\theta : M \to F$ with $\phi\theta = 1_M$. Factoring out P, ϕ and θ induce inverse isomorphisms between F/PF and M/PM, so $\theta(M) + PF = F$ and

$\theta(M) = F$ by Nakayama's lemma. Thus $\theta : M \to \theta(M) \oplus \operatorname{Ker}\phi$ is surjective. It follows that $\operatorname{Ker}\phi = 0$ and ϕ is an isomorphism. Thus M is free.
(b) Assume M is finitely generated. The module M is projective if and only if for all exact sequences $B \to C \to 0$ the sequence $\operatorname{Hom}_R(M, B) \to \operatorname{Hom}_R(M, C) \to 0$ is exact. If this is so, then because localization is exact and by 2.10, $\operatorname{Hom}_{R[U^{-1}]}(M[U^{-1}], B[U^{-1}]) \to \operatorname{Hom}_{R[U^{-1}]}(M[U^{-1}], C[U^{-1}]) \to 0$ is exact, and every epimorphism has the form $B[U^{-1}] \to C[U^{-1}] \to 0$, so $M[U^{-1}]$ is projective. Conversely, if all such locallized sequences at maximal ideals are exact then so is $\operatorname{Hom}_R(M, B) \to \operatorname{Hom}_R(M, C) \to 0$, because (by another result) it is the intersection of the localizations at the maximal ideals, so if M is projective on localization at all maximal ideals, it is projective.

5. (4.20 of Eisenbud) For each $n \in \mathbb{Z}$, find the integral closure of $\mathbb{Z}[\sqrt{n}]$ as follows:
(a) Reduce to the case where n is square-free.
(b) $\sqrt{n}$ is integral, so what we want is the integral closure R of $\mathbb{Z}$ in the field $\mathbb{Q}[\sqrt{n}]$. If $\alpha = a + b\sqrt{n}$ with $a, b \in \mathbb{Q}$, then the minimal polynomial of α is $x^2 - \operatorname{Trace}(\alpha)x + \operatorname{Norm}(\alpha)$ where $\operatorname{Trace}(\alpha) = 2a$ and $\operatorname{Norm}(\alpha) = a^2 - b^2n$. Thus $\alpha \in R$ if and only if $\operatorname{Trace}(\alpha)$ and $\operatorname{Norm}(\alpha)$ are integers.
(c) Show that if $\alpha \in R$ then $a \in \frac{1}{2}\mathbb{Z}$. If $a = 0$, show $\alpha \in R$ iff $b \in \mathbb{Z}$. If $a = \frac{1}{2}$ and $\alpha \in R$, show that $b \in \frac{1}{2}\mathbb{Z}$. Thus, subtracting a multiple of $\sqrt{n}$, we may assume $b = 0$ or $\frac{1}{2}$. Observe $b = 0$ is impossible.
(d) Conclude that the integral closure is $\mathbb{Z}[\sqrt{n}]$ if $n \not\equiv 1 \pmod 4$, and is $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{n}]$ if $n \equiv 1 \pmod 4$.

Solution. (a) If $n = p^2n'$ for some integers p and n' then $\mathbb{Z}[\sqrt{n}]$ and $\mathbb{Z}[\sqrt{n}']$ have the same field of fractions and integral closure (because $\sqrt{n}$ and $\sqrt{n}'$ are both integral over $\mathbb{Z}$), so we can assume n is square-free.
(b) We accept many of the assertions made in the question. Thus the minimal polynomial of α has that form because it equals $(x - (a + b\sqrt{n}))(x - (a - b\sqrt{n}))$. Also if $\operatorname{Trace}(\alpha)$ and $\operatorname{Norm}(\alpha)$ are integers then $\alpha \in R$ because it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. Conversely, if $\alpha \in R$ it is a root of a monic polynomial $f(x) \in \mathbb{Z}[x]$ of which the minimal polynomial $x^2 - \operatorname{Trace}(\alpha)x + \operatorname{Norm}(\alpha)$ is a factor in $\mathbb{Q}[x]$. By Gauss's Lemma the minimal polynomial has integer coefficients.
(c) If $\alpha \in R$ then $\operatorname{Trace}(\alpha) = 2a$ is an integer, so $a \in \frac{1}{2}\mathbb{Z}$. If $a = 0$ and $b \in \mathbb{Z}$ then $\alpha^2 - b^2n = 0$ so α is integral. If $a = 0$ and $b \notin \mathbb{Z}$ then the minimal polynomial $\alpha^2 - b^2n$ does not have coefficients in $\mathbb{Z}$ because n is square-free, so α is not integral. If $a = \frac{1}{2}$ and $\alpha \in R$ then, because $\operatorname{Norm}(\alpha) = a^2 - b^2n = \frac{1}{4} - b^2n \in \mathbb{Z}$, we deduce that $b \in \frac{1}{2}\mathbb{Z}$. The integrality of α is unchanged on adding or subtracting integer multiples of $\sqrt{n}$, so to determine the possibilities for b when $a = \frac{1}{2}$ it suffices to assume $b = 0$ or $\frac{1}{2}$. If $b = 0$ we get $\alpha = \frac{1}{2}$, which is not integral, so $b = 0$ is impossible.
(d) From (c) we see that if the integral closure is larger than $\mathbb{Z}[\sqrt{n}]$ then it must be $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{n}]$ because any integral element $a + b\sqrt{n}$ not in $\mathbb{Z}[\sqrt{n}]$ must have a, b not in $\mathbb{Z}$ and with denominator 2, and all such elements are equivalent to $\frac{1}{2} + \frac{1}{2}\sqrt{n}$ by adding

elements of $\mathbb{Z}[\sqrt{n}]$. Now $\frac{1}{2}+\frac{1}{2}\sqrt{n}$ is integral if and only if $\frac{1}{4}-\frac{1}{4}n=\frac{1-n}{4}\in\mathbb{Z}$, which means $n\equiv 1 \pmod 4$.

6. (1.3 of Matsumura plus) Let A and B be rings, and $f: A\to B$ a surjective homomorphism.
(a) Prove that $f(\operatorname{Jac} A)\subseteq \operatorname{Jac} B$, and construct an example where the inclusion is strict.
(b) Prove that if A is a semilocal ring (a ring with only finitely many maximal ideals) then $f(\operatorname{Jac} A)=\operatorname{Jac} B$.
(c) Continue to assume that A is a semilocal ring. Show that, as an A-module, $A/\operatorname{Jac}(A)$ is a direct sum of finitely many simple A-modules, and that $\operatorname{Jac}(A)$ is the smallest ideal with this property. (That is, if J is an ideal so that A/J is a direct sum of simple A-modules, then $J\supseteq \operatorname{Jac}(A)$.)

Solution. (a) If.I is a maximal ideal of B then $f^{-1}(I)$ is a maximal ideal of A by the correspondence theorem for surjective maps. Thus if $r\in\operatorname{Jac}(A)$ then $r\in f^{-1}(I)$, so $f(r)\in I$. Since I was arbitrary, $f(r)\in\operatorname{Jac}(B)$, so $f(\operatorname{Jac} A)\subseteq\operatorname{Jac} B$. Consider the example $A=\mathbb{Z}$ and $B=\mathbb{Z}/4\mathbb{Z}$ where $\operatorname{Jac}(A)=0$ and $\operatorname{Jac}(B)=2\mathbb{Z}/4\mathbb{Z}$, so the containment is strict.
(b) We will show that $B/f(\operatorname{Jac}(A)=f(A/\operatorname{Jac}(A))$ has Jacobson radical 0. From this it will follow that $\operatorname{Jac}(B)=f(\operatorname{Jac} A)$ because, by part (a) applied to the quotient homomorphism $B\to B/f(\operatorname{Jac} A)$, we have $\operatorname{Jac}(B)+f(\operatorname{Jac}(A))\subseteq f(\operatorname{Jac}(A))$ and we already know $\operatorname{Jac}(B)\supseteq f(\operatorname{Jac}(A))$. Now $\operatorname{Jac}(A)$ is the intersection of finitely many maximal ideals $I_1,\ldots,I_t$, so the Chinese Remainder Theorem (extended by induction to the case of more than 2 ideals) implies that $A/\operatorname{Jac} A\cong A/I_1\times\cdots\times A/I_t$ is a product of fields. The only ideals in such a ring are the products of certain of the fields, so $f(A/\operatorname{Jac}(A))$ is also a product of fields. This has Jacobson radical 0 because the maximal ideals are products of all except one of the fields, and such ideals intersect in 0.
(c) In the expression $A/\operatorname{Jac} A\cong A/I_1\times\cdots\times A/I_t$ from part (b), each field is a simple A-module, which establishes the first statement. If J is an ideal of A with the property that $A/J=S_1\oplus\cdots\oplus S_t$ is a direct sum of simple modules, let I_n be the preimage in A of $\cdots S_{n-1}\oplus 0\oplus S_{n+1}\cdots$ where S_n is omitted from the direct sum. Then I_n is a maximal ideal of A and $\bigcap_{n=1}^t I_n=J$. It follows that $J\supseteq\operatorname{Jac}(A)$.

Extra question: do not upload to Gradescope.

7. Show that the Jacobson radical of $k[x_1,\ldots,x_n]$ is 0.