2014 Algebra SEP $\sim$ Standard Rings and Modules Facts (by Evan Dummit)

- Suggested reading:
  - Basic rings: Dummit/Foote chapters 7-9.
  - Modules: Dummit/Foote sections 10.1-10.3.
  - Integrality / radicals / primary ideals / Noetherian conditions: Dummit/Foote sections 15.2-15.4, 16.1.
  - Tensor products and exact sequences: Dummit/Foote sections 10.4-10.5.
- Examples you should be familiar with:
  - Commutative rings: fields, $\mathbb{Z}$, quadratic integer rings $\mathbb{Q}[\sqrt{D}]$ for an integer D, polynomial rings in a (possibly infinite) number of variables, formal power series rings.
  - Noncommutative rings: matrix rings, group rings.
  - Modules: vector spaces, R/I as an R-module, abelian groups as $\mathbb{Z}$-modules, free modules, pairs (V, T) as $F[x]$-modules (where V is an F-vector space and $T : V \to V$).
- Basic rings properties:
  - Rings usually have a 1, and are sometimes commutative. Be aware of the differences between commutative and noncommutative rings.
  - A subring S of R is an additive subgroup of R closed under multiplication.
  - A (left, right, two-sided) ideal I of R is an additive subgroup of R closed under (left, right, both) multiplication by arbitrary elements of R. Ideals are the kernels of ring homomorphisms.
  - Isomorphism theorems for rings:
    - First isomorphism theorem: If $\varphi : R \to S$ is a homomorphism, then $\text{im}(\varphi) \cong R/\ker(\varphi)$.
    - Second isomorphism theorem: If A is a subring and B is an ideal, then $(A + B)/B \cong A/(A \cap B)$.
    - Third isomorphism theorem: If $I \subseteq J$ are ideals, then $(R/I)/(J/I) \cong R/J$.
    - Lattice isomorphism theorem: If I is an ideal, the ideals (subrings) of R/I are in bijection with the ideals (subrings) of R containing I.
  - A zero divisor is a nonzero element $x \in R$ such that there exists a nonzero $y \in R$ with $xy = 0$.
  - A nilpotent element is an element $x \in R$ such that there exists an n with $x^n = 0$.
    - If R is commutative, the set of nilpotent elements forms an ideal, called the nilradical.
  - A unit is an element $x \in R$ such that there exists $y \in R$ with $xy = yx = 1$.
    - A ring is a division ring if every nonzero element is a unit. A commutative division ring is a field.
  - A ring is an integral domain (or just a domain) if it is commutative, has a 1, and has no zero divisors.
  - An idempotent is an element $e \in R$ such that $e^2 = e$.
  - An ideal M is maximal if it is proper and there are no other proper ideals containing it. If R is commutative with 1, I is maximal if and only if R/I is a field.
    - If R has a 1, every ideal is contained in a maximal ideal by a standard Zorn's lemma argument.
  - An ideal P is prime if $xy \in P$ implies either $x \in P$ or $y \in P$. If R is commutative with 1, I is prime if and only if R/P is an integral domain.
  - An ideal I is principal if it can be generated by 1 element – i.e., if $I = (d)$ for some $d \in R$.
  - An integral domain R is a principal ideal domain (PID) if every ideal of R is principal.
    - $\mathbb{Z}$ and $F[x]$ are PIDs. $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Z}[x]$ are not PIDs.
  - In a domain, a nonzero non-unit element $x \in R$ is irreducible if any factorization $yz = x$ has either y or z a unit.
  - In a domain, a nonzero element $x \in R$ is prime if (x) is a prime ideal. Prime elements are irreducible.
  - In a domain, two elements $a, b \in R$ are associates if $a = bu$ for some unit u.

- An integral domain R is a unique factorization domain (UFD) if every element of R can be factored uniquely (up to associates and reordering) into irreducible elements.
  - PIDs are UFDs. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.
- If R is commutative with 1 and D is any multiplicatively-closed subset containing 1, then the set of elements $D^{-1}R$ given by elements of the form $\frac{r}{d}$ with $r \in R$ and $d \in D$, subject to the equivalence relation $r/d = r'/d'$ if $q(rd' - r'd) = 0$ for some nonzero $q \in R$, is called the localization of R at D.
  - The localization is easier-defined via the universal property: there exists a map $\varphi : R \to D^{-1}R$ such that if $\psi : R \to S$ is any ring homomorphism sending 1 to 1 such that $\psi(d)$ is a unit for every $d \in D$, then there is a unique homomorphism $\Psi : D^{-1}R \to S$ such that $\Psi \circ \varphi = \psi$. In other words, the localization is the ring obtained by declaring that all elements of D are units.
  - If R is a domain the definition is simpler, and in the further special case where $D = R\backslash\{0\}$, the localization $D^{-1}R$ is called the field of fractions of R, as it consists of the elements $\frac{r_1}{r_2}$ where $r_2 \neq 0$, and is the smallest field containing R. (The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$, for example.)
- A commutative ring with 1 is Noetherian if every ideal is finitely-generated; equivalently, if every ascending chain of ideals of R is eventually constant.
- A commutative ring with 1 is Artinian if every descending chain of ideals of is eventually constant.
- A commutative ring with 1 is a local ring if it has a unique maximal ideal. A ring is a local ring if and only if the maximal ideal consists of all nonunits of R.
- (Chinese Remainder Theorem) If $A_1, \cdots, A_k$ are pairwise-comaximal ideals of R (i.e., with $A_i + A_j = R$ for $i \neq j$), then $R/(A_1 \cdots A_k) \cong (R/A_1) \times \cdots \times (R/A_k)$.
- (Gauss's Lemma) If R is a UFD with field of fractions F, then a polynomial $p(x) \in R[x]$ is reducible in $R[x]$ iff it is reducible in $F[x]$.
  - Corollary: If R is a UFD, then $R[x]$ is a UFD.
- (Eisenstein's Criterion) If $f(x) \in R[x]$ is a monic polynomial and R is a domain, and all coefficients of $f(x)$ except for the leading term lie in a prime ideal P, but the constant term of $f(x)$ does not lie in P^2, then $f(x)$ is irreducible in $R[x]$.
- (Hilbert Basis Theorem) If R is Noetherian, then so is $R[x]$.

- Basic modules properties:
  - If M, N are R-modules, then $\mathrm{Hom}_R(M, N)$ is the R-module of homomorphisms from M to N. We call $\mathrm{Hom}_R(M, M)$ the endomorphism ring of M (since it carries a ring structure, namely composition).
    - A module M is simple if it has no proper nontrivial submodules.
    - (Schur's Lemma) The endomorphism ring of a simple module is a division ring.
  - Isomorphism theorems for modules:
    - First isomorphism theorem: If $\varphi : M \to N$ is a homomorphism, then $\mathrm{im}(\varphi) \cong M/\ker(\varphi)$.
    - Second isomorphism theorem: If A and B are submodules of M, then $(A + B)/B \cong A/(A \cap B)$.
    - Third isomorphism theorem: If $A \subseteq B$ are submodules of M, then $(M/A)/(B/A) \cong M/B$.
    - Lattice isomorphism theorem: If A is an submodule of M, the submodules of M/A are in bijection with the submodules of M containing A.
  - A module M is cyclic if it is generated by one element; namely, if $M = Ra$ for some $a \in M$.
  - A module M is finitely-generated if it is generated by a finite collection of elements; namely, if $M = Ra_1 + Ra_2 + \cdots + Ra_n$ for some $a_1, \cdots, a_n \in M$.
  - A module F is free on a subset A of F if for every nonzero $x \in F$ there exist unique $r_1, \cdots, r_n \in R$ and unique $a_1, \cdots, a_n \in A$ such that $x = r_1 a_1 + \cdots + r_n a_n$.
    - (Universal property of free modules) For any set A there is a free R-module $F(A)$, and if M is any other R-module and $\varphi : A \to M$ is a map of sets, then φ extends uniquely to an R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \varphi(a)$ for all $a \in A$.

  - A module is Noetherian if every submodule is finitely-generated; equivalently, if every ascending chain of submodules is eventually constant; equivalently, if every nonempty set of submodules contains a maximal element.
    - The definition of Noetherian ring (above) is simply saying that R is a Noetherian module over itself.
  - If M is a module over a commutative ring, then its torsion submodule is defined as $\mathrm{Tor}(M) = \{x \in M : rx = 0$ for some and the rank of M is the maximal number of R-linearly independent elements of M.
  - (Structure Theorem for finitely-generated modules over PIDs) If M is a finitely-generated module over the PID R, then $M \cong R^d \oplus \mathrm{Tor}(M)$, where d is the rank of M, and moreover $\mathrm{Tor}(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_n)$ for uniquely-defined (up to associates) nonzero nonunits $a_1, \cdots, a_n \in R$ with $a_1 | a_2 | \cdots | a_n$.

- Facts about radical ideals / primary ideals / Jacobson radical (assume R is commutative and has a 1):
  - If I is an ideal, the radical of I is defined as $\mathrm{rad}(I) = \left\{a : a^k \in I \text{ for some } k \geq 1\right\}$.
    - An ideal I is radical if $I = \mathrm{rad}(I)$.
    - The radical of I is the intersection of all prime ideals containing I. In particular, prime ideals are radical.
    - If R is Noetherian, then there exists some $k \geq 1$ for which $[\mathrm{rad}(I)]^k \subseteq I$.
  - The nilradical is the radical of the zero ideal. Hence, the nilradical is the intersection of all prime ideals of R.
  - A proper ideal Q is primary if $xy \in Q$ implies $x \in Q$ or $y^n \in Q$ for some $n \geq 1$. Equivalently, Q is primary if $ab \in Q$ and $a \notin Q$ implies $b \in \mathrm{rad}(Q)$.
    - Prime ideals are primary.
    - An ideal Q is primary iff every zero divisor in R/Q is nilpotent.
    - The radical of a primary ideal is prime, and it is the unique smallest prime ideal containing Q. This prime ideal is called the associated prime to Q.
  - An ideal I has a primary decomposition if it can be written as a finite intersection of primary ideals. A primary decomposition is minimal if no primary ideal contains the intersection of all the others, and the associated primes are all distinct.
    - (Lasker-Noether) In a Noetherian ring, every proper ideal has a minimal primary decomposition. Further, if $I = \bigcap Q_i = \bigcap Q_i'$ has two minimal decompositions, then the sets of associated primes $\{\mathrm{rad}(Q_i)\}$ and $\{\mathrm{rad}(Q_i')\}$ for the two decompositions are the same, and the primary components belonging to minimal elements in the set of associated primes are uniquely determined. (In general the minimal decomposition itself is not unique.)
  - The Jacobson radical $\mathrm{Jac}(R)$, sometimes $J(R)$ or just J, is the intersection of all maximal ideals of R.
    - If I is a proper ideal, then $I + \mathrm{Jac}(R)$ is also a proper ideal.
    - An element x belongs to $\mathrm{Jac}(R)$ if and only if $1 - rx$ is a unit for all $r \in R$.
    - (Nakayama's Lemma) If M is a finitely-generated R-module and $M = \mathrm{Jac}(R)M$, then $M = 0$.
    - If R is Artinian (and commutative with 1) then $R/\mathrm{Jac}(R)$ is isomorphic to a finite direct product of fields. In particular, R is isomorphic to a finite direct product of Artinian local rings.

- Facts about integrality and algebraic integers:
  - If R is a subring of the commutative ring S sharing the same 1, $s \in S$ is integral over R if s satisfies a monic polynomial in $R[x]$. Equivalently, s is integral over R if $R[s]$ is a finitely-generated R-module.
    - If every element of S is integral over R, S is an integral extension of R.
    - The integral closure of R in S is the set of elements of S that are integral over R. (By the module criterion for integrality, we see that the integral closure of R is a subring of S.)
    - If R equals its integral closure in R, we say R is integrally closed in S. Important note: a domain is called integrally closed (with no modifying ring) if it is integrally closed in its field of fractions.
    - Integrality is transitive: if T is integral over S and S is integral over R, then T is integral over R.
    - A UFD is integrally closed in its field of fractions. An example of a non-integrally-closed ring is $F[x, y]/(y^2 - x^3)$; its integral closure contains y/x.

  - If $K/\mathbb{Q}$ is a field extension, then $\alpha \in K$ is an algebraic integer if α is integral over $\mathbb{Z}$. The integral closure of $\mathbb{Z}$ in K, denoted $\mathcal{O}_K$, is called the ring of integers of K.
    - An element $\alpha \in \bar{\mathbb{Q}}$ is an algebraic integer if and only if the coefficients of its minimal (monic) polynomial are integers.
    - By the integrality properties, we see that the sum, difference, and product of algebraic integers is also an algebraic integer.
    - If $|K : \mathbb{Q}| = n$, then $\mathcal{O}_K$ is a Noetherian ring and a free $\mathbb{Z}$-module of rank n, and the field of fractions of $\mathcal{O}_K$ is K.

- Facts about tensor products (continue assuming that R is commutative with 1):
  - If M and N are two R-modules, then the tensor product $M \otimes_R N$ is defined to be the R-module whose elements are sums of "simple tensors" of the form $m \otimes n$ where $m \in M$, $n \in N$, subject to the R-module relations (i) $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$, (ii) $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$, and (iii) $r(m \otimes n) = (rm) \otimes n = m \otimes (rn)$.
  - A map $\varphi : M \times N \to L$ is called R-bilinear if it is R-linear in each component – i.e., $\varphi(m_1 + rm_2, n) = \varphi(m_1, n) + r\varphi(m_2, n)$ and $\varphi(m, n_1 + rn_2) = \varphi(m, n_1) + r\varphi(m, n_2)$.
  - (Universal property of tensor products) If L is any R-module, then there is a bijection between the set of R-bilinear maps $\varphi : M \times N \to L$ and the R-module homomorphisms $\Phi : M \otimes_R N \to L$.
    - The action of Φ is simply that of φ extended linearly from simple tensors; the R-bilinearity ensures this is well-defined on the tensor product.
  - It is generally difficult to prove that any particular tensor product is nonzero directly from the definition: to show the existence of some nonzero elements in a tensor product, it is easiest to use the universal property instead, by constructing an appropriate and nonzero R-bilinear map out of $M \times N$.
  - Tensor products are associative: $(M \otimes_R N) \otimes_S L \cong M \otimes_R (N \otimes_S L)$, provided everything makes sense. (One can prove this by defining the appropriate notion of an "R,S-trilinear map", which also generalizes naturally to general "multilinear" maps having the analogous universal property.)
  - Tensor products commute with arbitrary direct sums.

- Useful tricks:
  - In general, if one has an ideal in a ring (or a submodule of a module), it is a good idea to look at the quotient ring (or module).
  - For example, in a commutative ring with 1, I is prime iff R/I is a domain and I is maximal iff R/I is a field. These properties are obvious but surprisingly useful.
  - For problems involving radicals or primary ideals, element-wise calculations are usually called for, unless there is a natural way to invoke Lasker-Noether.
  - For problems involving integrality, it is usually a good idea to think about the monic polynomial satisfied by an integral element.
  - For problems involving tensor products, to show some element in a tensor product is zero, one can usually do element-wise calculations. However, to establish that some particular tensor product is nonzero, it is almost always necessary to invoke the universal property. Also, make sure that you don't fall into the trap of forgetting about non-simple tensors: most elements in a tensor product are not simple tensors!
  - For problems involving Noetherian (or Artinian) rings or modules, the idea is usually to construct some increasing (or decreasing) chain of ideals or submodules, and then use the stabilization property.
  - For problems involving exact sequences, injective/projective/flat modules, or several module homomorphisms (or similar things), diagram-chasing is often necessary. This means, roughly: draw a commutative diagram of all the modules and homomorphisms, and then pick an appropriate element (or elements) in one of the modules and "chase" the element around the diagram by applying the various maps (either directly, or by taking inverse images).
  - On the most recent qualifying exams, there has usually been one problem on tensor products / exact sequences, and often (though not always) a second problem on the other ring theory topics.