Lecture Notes of the Algebra Group at Dokuz Eylül University Department of Mathematics: Wedderburn-Artin Theorem (an extended version)

Mistakes survive all corrections; nevertheless, point out if you run into one.

THEOREM 1. The following conditions are equivalent for a ring R.

(i) R_R is semisimple,
(ii) $J(R) = 0$ and R is right Artinian,
(iii) R is semiprime (i.e. R has no nonzero nilpotent ideals) and right Artinian,
(iv) $R \cong \prod_{i=1}^{n} M_n(D_i)$, where D_i are some division rings,
(v) Every right R-module is semisimple,
(vi) Every (simple) right R-module is projective,
(vii) Every right R-module is injective,
(viii) The left-hand-side versions of the above statements.

From a historical viewpoint one could say that the equivalence $(i) \Leftrightarrow (ii) \Leftrightarrow (iv)$ is the core of the theorem, and the rest is periphery. As we divide the proof into several lemmas and propositions, we will also utilize the context to give some background information about ring and module theory. Concepts recently defined in class will be recalled as we go along.

LEMMA 1. Let M be a module. If I is a family of simple submodules of M such that $M = \sum_{B \in I} B$ and A is a submodule of M, then there exists some $I' \subseteq I$ such that $M = (\bigoplus_{B \in I'} B) \oplus A$.

Sketch of Proof. As we have seen in class, the set of such sub-families Γ of I as satisfy $\sum_{B \in \Gamma} B + A = (\bigoplus_{B \in \Gamma} B) \oplus A$ is an inductive set (every chain in it has an upper bound), so that, by Zorn's Lemma, it has a maximal element say I'. One only needs to verify that if the sum $(\bigoplus_{B \in I'} B) \oplus A$ were not equal to M, it would have to have zero intersection with some $C \in I$, whence it would be easy to see that the family $I' \cup \{C\}$ would contradict the maximality of I'. Now, the conclusion follows.

DEFINITION 1. Given a module M we will call the sum of all simple submodules of M the socle of M and denote it by $soc(M)$.

COROLLARY 1. A module M is semisimple if and only if every submodule of M is a direct summand of M, i.e. for any $A \leq M$, there exists some $H \leq M$ such that $M = A \oplus H$.

Proof. $(\Rightarrow)$ follows from Lemma 1. Assume, conversely, that every submodule of M is a direct summand of M. Then $soc(M) \oplus B = M$ for some $B \leq M$. If $B \neq 0$, then we can choose a nonzero cyclic submodule A of B. By Zorn's Lemma, A has a maximal submodule, say C. C is a direct summand of M by assumption. So $C \oplus C' = M$ for some $C' \leq M$. By modular law, $A = C \oplus (A \cap C')$, so that $\frac{A}{C} \cong A \cap C'$ is a simple submodule of A, and hence of M, contradicting the fact that $(A \cap C') \cap soc(M) \subseteq B \cap soc(M) = 0$. This means that $B = 0$, so that $M = soc(M)$ is semisimple.

LEMMA 2. If M is semisimple and $A \leq M$, then A and $\frac{M}{A}$ are semisimple.

Proof. Every submodule of M is semisimple by Corollary 1 and modular law. Furthermore, for any $A \leq M$, there is some $B \leq M$ such that $M = A \oplus B$ (again by Corollary 1), so that $\frac{M}{A} \cong B$. Since B is semisimple, so is $\frac{M}{A} \cong B$.

QUESTION 1. Is the converse Lemma 2 true?

DEFINITION 2. A free (right) module over a ring R is one that is isomorphic to a direct sum of copies of R_R. For example, R_R itself is free, and so is $R \oplus R$ as a right R-module.

PROPOSITION 1. Every module is (isomorphic to) a factor of a free module.

Proof. Let M be a module and consider the map $\bigoplus_{m \in M} R_R \to M$ defined by the rule $f((r_m)_{m \in M}) = \sum_{m \in M, r_m \neq 0} m r_m$. It is routine to verify that f is an epimorphism, proving our assertion.

COROLLARY 2. If R_R is semisimple, then so is every right R-module.

Proof. The assertion immediately follows from Lemma 2 and Proposition 1.

DEFINITION 3. A module M is said to be an injective module if, for any monomorphism $f : M \to N$, $f(M)$ is a direct summand of N. For example, $\mathbb{Q}_{\mathbb{Z}}$ and the Prüfer group $\mathbb{Z}_{p^\infty}$ are injective $\mathbb{Z}$-modules. Dually, M is called a projective module if the kernel of every epimorphism $N \to M$ is a direct summand of N.

COROLLARY 3. R_R is semisimple if and only if every right R-module is injective if and only if every right module is projective.

Proof of the first equivalence. ($\Rightarrow$) If R_R is semisimple then every right R-module is semisimple by Corollary 2. Then, given any homomorphism $f : M \to N$ between any two (right) modules M and N, $f(M)$, being a submodule of N, is a direct summand of N by Corollary 1.

($\Leftarrow$) For any right ideal A of R, the inclusion map $A \to R$ splits by assumption, i.e. its image A is a direct summand of R_R. This implies by Corollary 1 that R_R is semisimple.

The proof for the second equivalence above is similar.

QUESTION 2. Prove the following assertions:

(a) If $f : A \to B$ and $g : B \to C$ are two homomorphisms such that gf is an isomorphism, then $Im(f) \oplus Ker(g) = B$.
(b) $f : M \to N$ is a monomorphism and $f(M)$ is a direct summand of N if and only if there exists a homomorphism $g : N \to M$ such that $gf = 1_M$.
(c) $g : N \to M$ is an epimorphism and $Ker(g)$ is a direct summand of N if and only if there exists a homomorphism $f : M \to N$ such that $gf = 1_M$.
(d) If R is a ring then R_R is projective.
(e) Direct sums and summands of projective modules are projective.
(f) Free modules are projective.
(g) If M is a projective module then it is isomorphic to a direct summand of a free module.
(h) Conclude from the above assertions that projectives are up to isomorphism precisely direct summands of free modules.

Notice that we have thus far established the equivalences $(i) \Leftrightarrow (v) \Leftrightarrow (vi) \Leftrightarrow (vii)$ of Theorem 1. The work in the sequel concerns the remaining and rather more ring theoretic part of Theorem 1, some of which happens to still be susceptible of a module theoretic approach; so we continue our discussion with the concept of a radical of a module with a prospect of applying it in a ring theoretic setting. In group theory, this corresponds to the Frattini subgroup. Recall that the Frattini subgroup of a group G is precisely the subgroup generated by its non-generators. We will prove the module theoretic version of this fact.

DEFINITION 4. Given a module M we define the radical of M, denoted $rad(M)$ to be the intersection of all of its maximal submodules, if they do exist; in case they do not, then $rad(M)$ is defined to be M itself. A submodule A of M is said to be a small submodule if, for any $B \leq M$, $A + B = M$ implies that $B = M$.

One can easily verify that any finite sum of small submodules of a module M is again a small submodule, and that any small submodule of a submodule of M is a small submodule of M.

QUESTION 3. Let $f : M \to N$ be a module homomorphism, $\{A_i : i \in I\}$ be a family of submodules of M and $\{B_j : j \in J\}$ be a family of submodules of N. Prove the following statements:

(1) $f(\sum_{i\in I} A_i) = \sum_{i\in I} f(A_i)$ and $f^{-1}(\bigcap_{j\in J} B_j) = \bigcap_{j\in J} f^{-1}(B_j)$,
(2) $f(\bigcap_{i\in I} A_i) \subseteq \bigcap_{i\in I} f(A_i)$ and $\sum_{j\in J} f^{-1}(B_j) \subseteq f^{-1}(\sum_{j\in J} B_j)$,
(3) In (2), the first equality holds if $Ker(f) \subseteq A_i$ for all $i \in I$, and the second one does if $B_j \subseteq Im(f)$ for all $j \in J$.

LEMMA 3. The following hold for any module M:

(i) $rad(M)$ is the submodule of M generated by (i.e. is the sum of) the small cyclic submodules of M (and thus contains all small submodules).
(ii) For any homomorphism $f : M \to N$, $f(A)$ is small in N whenever A is small in M.
(iii) For any homomorphism $f : M \to N$, $f(rad(M)) \subseteq rad(N)$.

Proof. (i) Let A be a small submodule of M and N be a maximal submodule. If A were not contained in N we would have $N + A = M$ by maximality of N, contradicting the smallness of A. So any small submodule is contained in any maximal submodule, whence $rad(M)$ contains the sum of small submodules.

Conversely, assume A is a cyclic submodule of $rad(M)$ that is not small. Then, the set S of proper submodules of M whose sum with A is equal to M is a nonempty set as well as an inductive one (how so?), so that S has a maximal element, say N. We will see that N is actually a maximal submodule of M: Else, there would be some C such that $N \subset C \subset M$. By maximality of N in S and since $C + A = M$, C must be a non-proper submodule, namely $C = M$, a contradiction. Thus, N is a maximal submodule of M not containing A. This means that $A \nsubseteq rad(M)$, proving that cyclic submodules of $rad(M)$ are small submodules of M, establishing the reverse inclusion, as desired.

(ii) Let A be a small submodule of M and assume that $f(A)+B = N$. Then, by modular law, $Im(f) = f(A)+(Im(f)\cap B)$. By Question 3 (iii), $M = f^{-1}(f(A))+ f^{-1}(Im(f)\cap B) = A+Ker(f)+f^{-1}(Im(f)\cap B) = A+f^{-1}(Im(f)\cap B)$, implying, by smallness of A, that $M = f^{-1}(Im(f) \cap B)$. But then, $Im(f) \subseteq B$, whence $B = N$, as desired.

(i) follows from (i), (ii) and Question 3.

QUESTION 4. Prove that if M is a finitely generated module then $rad(M)$ is a small submodule of M.

COROLLARY 4. For a ring R, $rad(R_R)$ and $rad({}_RR)$ are ideals.

Proof. It suffices to verify that the former is a left ideal, the proof for the latter will follow by symmetry: For any $r \in R$, $r \cdot rad(R_R)$ is the image of $rad(R_R)$ under the R-linear map $R \to R$ induced by left multiplication by r, whence $r \cdot rad(R_R) \subseteq rad(R_R)$ by Lemma 3.

QUESTION 5. Prove that if M is a right module over a ring R and $J = rad(R_R)$, then $MJ \subseteq rad(M)$.

PROPOSITION 2. If M is an Artinian module with $rad(M) = 0$, then M is semisimple.

Proof. Let $A \leq M$. Since M is Artinian and $A + M = M$, one can choose a submodule B of M minimal with respect to the property that $A + B = M$. Now we claim that $A \cap B$ is a small submodule of B, whence of M: If $(A \cap B) + C = B$, then $A + C = M$. By minimality of B as chosen, $C = B$, proving the claim. Thus, by assumption $A \cap B \subseteq rad(M) = 0$, and consequently $A \oplus B = M$. This shows that any submodule of M is a direct summand of M, yielding that M is semisimple.

Remark that any semisimple module has zero radical.

PROPOSITION 3. If R is a ring then
(i) $rad(R_R)$ is the largest right ideal I such that $1 - a$ is (right) invertible for each $a \in I$, and
(ii) $rad(R_R) = rad({}_RR)$.

Proof. (i) Since, for each $a \in J$, aR is a small right ideal of R and $aR + (1 - a)R = R$, we have $(1 - a)R = R$, so that $(1 - a)$ is right invertible, whence there is some $b \in R$ such that $(1 - a)b = 1$. Then $1 - b = -ab \in rad(R_R)$, and the same argument as above with a replaced by $1 - b$ yields that b is right invertible. So $bc = 1$ for some $c \in R$. Then $1 - a = (1 - a)bc = c$, making $(1 - a)$ invertible. Thus, J satisfies the said property. Now assume that I is an ideal such that for any $a \in I$ $1 - a$ is right invertible. If $a \in I$ and $aR + B = R$, then there exist $r \in R$ and $b \in B$ such that $1 = ar + b$. By assumption, $b = 1 - ar$ is right invertible, so that $bR = R$, whence $B = R$, proving that aR is a small right ideal, forcing $aR \subseteq rad(R_R)$ by Lemma 3. Thus, $I \subseteq rad(R_R)$.
(ii) By (i) and Corollary 4, $rad({}_RR)$ is a right ideal such that for every $a \in rad({}_RR)$, $1 - a$ is invertible, implying, again by (i), that $rad({}_RR) \subseteq rad(R_R)$. The reverse inclusion follows by symmetry of our arguments.

DEFINITION 5. For any ring R, $rad(R_R) = rad({}_RR)$ is called the Jacobson radical of R. We will henceforth drop the notation rad for the radical of a ring and just use J (or $J(R)$ when the context necessitates the discernment of the ring R) instead.

PROPOSITION 4. If R is a right Artinian ring, then J is nilpotent and the ring $\overline{R} = \frac{R}{J}$ is a semisimple right $\overline{R}$-module.

Proof. By assumption the chain $J \supseteq J^2 \supseteq J^3 ...$ terminates, say, at the n^{th} step, i.e. $J^n = J^{n+1} = ...$ Assume, contrary to what we aim to prove, that $J^n \neq 0$. Then the set $S = \{I \leq R_R : IJ^n \neq 0\}$ contains J and is thus nonempty. Since R is right Artinian S has a minimal element, say A. There is some $a \in A$ such that $(aR)J^n = aJ^n = aJ^{n+1} \neq 0$. By minimality of A we have $A = aR = aJ = AJ$. But this is a contradiction since $AJ \subseteq rad(A)$ which is small in A, by Questions 4 and 5. Thus, J is nilpotent.

The right R-module structure and the right $\overline{R}$-module structure of the ring $\overline{R}$ coincide, and $\overline{R}_R$ is an Artinian module with zero radical. Thus, $\overline{R}_R$ is semisimple by Proposition 2, whence so too is $\overline{R}_{\overline{R}}$.

Before the next lemma, remark that a semisimple module is finitely generated iff it is Artinian iff it is Noetherian.

Lemma 4. Let R be ring with nilpotent Jacobson radical such that $\overline{R}_{\overline{R}}$ is semisimple, where $\overline{R} = \frac{R}{J}$. Then Noetherian modules and Artinian modules are the same class.

Proof. Let M be Artinian or Noetherian, and assume $J^n = 0$. Then the factors of the sequence $M \supseteq MJ \supseteq MJ^2 \supseteq .... \supseteq MJ^n = 0$, being right $\overline{R}$-modules, are finitely generated semisimple (why?) both as right $\overline{R}$-modules and as right R-modules. So, for example, if M is Noetherian, then both MJ^{n-1} and $\frac{MJ^{n-2}}{MJ^{n-1}}$ are Noetherian semisimple whence Artinian modules, implying that MJ^{n-2} is Artinian. Continuing in this manner one eventually concludes that M is Artinian. The proof that M being Artinian implies M being Noetherian is similar.

Proposition 4 and Lemma 4 immediately yield

Theorem 2. If R is a right Artinian ring then R is right Noetherian.

What is a counterexample to the converse of this theorem?

In linear algebra, a linear transformation on an n-dimensional vector space V over a field F is identified with an $n \times n$-matrix in a well-known way. In fact, this identification defines an isomorphism from the ring of linear transformations $V \to V$ to the ring $M_n(F)$. Looking from another point of view, such a vector space is isomorphic to F^n, and the ring of its linear transformations is isomorphic to $M_n(End(F_F))$; this is because of the ring isomorphism $End(F_F) \cong F$, which, we know, holds for any ring. We can think similarly for a module over an arbitrary ring, which is basically a vector space over that ring, and prove, in essentially the same way, the following:

Lemma 5. If $M \cong A^n$ for a module A, then $End(M) \cong M_n(End(A))$.

Question 6. Let $M \cong A \oplus B$, where $Hom(A, B) = 0$ and $Hom(B, A) = 0$. Show that there is a ring isomorphism $End(M) \cong End(A) \times End(B)$.

Definition 6. If M is a semisimple module, for each simple module S, we define the S-component of M to be the sum of all simple submodules of M isomorphic to S. If M has a single nonzero S-component for a simple module S, we call M a homogeneous semisimple module. An S-component is itself a homogeneous semisimple module, and is alternatively called a homogeneous component of M.

Question 7. Prove that any simple submodule of an S-component is isomorphic to S.

Question 8. Show that if R is a ring such that $R = A \oplus B$ where A and B are ideals, then the following hold:

(1) A and B are cyclic R-modules each generated by a central idempotent.
(2) If $A = eR$ for a central idempotent e of R, then A is a ring with identity e, and right(/left) ideals of A are precisely right(/left) ideals of R contained in A. Furthermore, if I is any right/left ideal of R, then I is the direct sum (as an R-module) of a right(/left) ideal of A and a right(/left) ideal of B.
(3) Right(/left) A-modules are precisely right(/left) R-modules annihilated by B. Every right R-module M has a decomposition into the direct sum of an A-module and a B-module.

Question 9. Prove that if M is a simple module then $End(M)$ is a division ring.

Question 10. Prove that a semisimple module is a direct sum of its homogeneous components.

Proposition 5. If R_R is semisimple, then R is isomorphic to a finite product of some matrix rings over division rings.

Proof. By Question 10, $R_R = H_1 \oplus ... \oplus H_n$, where H_i are homogeneous components of R_R. Assume, without loss of generality, that for each $i \in \{1, ..., n\}$, $H_i \neq 0$ and is the S_i-component of R_R with respect to some simple right R-module S_i. Then, for $i \neq j$, $Hom(H_i, H_j) = 0$. This implies that $H_j H_i = 0$, whence H_i are ideals and the above decomposition is a ring direct sum (i.e. H_i are ideals). It is easy to see that each H_i is a homogeneous semisimple right H_i-module. In fact, for each i, there is an H_i-linear (as well as R-linear) isomorphism $H_i \cong S_i^{k_i}$ for some k_i. Then, by Question 6 and Lemma 5, we have $R \cong End(R_R) \cong \prod_{i=1}^n End(H_i) \cong \prod_{i=1}^n M_{k_i}(End(S_i))$. Since each $End(S_i)$ is a division ring by Question 9, the conclusion follows.

Question 11. Let R be a ring. Prove that ideals of the matrix ring $M_n(R)$ are of the form $M_n(I)$, where I are ideals of R. Also show that the assertion does not hold for one-sided ideals.

Question 12. Let D be a division ring and $R = M_n(D)$. Then R is a simple ring, namely one that has no proper nonzero ideals, and the rows of R are simple right ideals isomorphic to each other, so that R_R is a homogeneous semisimple right R-module. Similarly, the columns are simple left ideals all isomorphic to each other, making ${}_RR$ a homogeneous semisimple left R-module.

Corollary 5. R_R is semisimple if and only if ${}_RR$ is semisimple.

Proof. Assume that R_R is semisimple. By Proposition 5, R is isomorphic, as a ring, to a finite direct product of matrix rings R_i over division rings. By Question 12, each R_i is also semisimple as a left R_i-module, meaning that each R_i is a direct sum of its simple left ideals. From the preceding statement, it is easy to see that R, too, is a direct sum of simple left ideals, yielding the conclusion.

Proof of Theorem 1: The equivalence of the conditions $(i), (v), (vi), (vii)$ were established as mentioned at the bottom of Page 2; $(ii) \Rightarrow (i)$ follows from Proposition 2, $(i) \Rightarrow (iv)$ from Proposition 5, $(iv) \Rightarrow (i)$ from Question 12, and the equivalence of $(viii)$ to the other conditions follows from Corollary 5. $(i) \Rightarrow (ii)$ follows from the remark preceding Lemma 4 and the fact that a semisimple module has no small submodules other than the zero submodule. The equivalence of (iii) to the other conditions is the subject of the next question.

DEFINITION 7. A ring of theorem 1 is alternately called a semisimple Artinian ring, a Wedderburn ring, or a simply a semisimple ring. The term "semisimple" in the phrase "semisimple Artinian ring" refers to Jacobson semisimplicity (namely the condition that $J(R) = 0$, and the sole use of it refers to R being semisimple as a (right as well as a left) module over itself.

QUESTION 13. Prove the following statements for a ring R:

(1) R is semiprime if and only if the intersection of all prime ideals of R is zero.
(2) Prove that a maximal ideal is prime.
(3) Notice that from our discussion above, it follows that a semisimple Artinian ring is a sum of simple rings, and that a simple ring has only one maximal ideal, namely the zero ideal.
(4) Prove that if R is semisimple Artinian, then R is semiprime.