MATH 7211 Homework 12

Andrea Bourque

May 9, 2023

1 Problem 18.2.11

Prove that if R is a ring with 1 such that every R-module is free, then R is a division ring.

Proof. Let I be a non-zero and proper (left, right, two-sided) ideal of R. Then R/I is naturally a non-zero R-module. By assumption, it is free, say with basis $\{x_j\}$. But for any $i \in I$, we have $ix_j = 0$ by definition of R/I. Thus R/I can't be free. It follows that the only ideals of R are 0 and $(1) = R$, i.e. R is simple.

Furthermore, any free module is also projective (depending on your definition of projective, this can be more or less obvious). Thus R satisfies the first condition of Wedderburn's theorem, meaning R is a direct product of two sided ideals which are isomorphic to matrix rings over division rings. By the previous observation, the only non-zero two-sided ideal of R is R, meaning R is a matrix ring over a division ring, say $M_n(\Delta)$. We want to prove that $n = 1$, so that $R = \Delta$.

We claim that for $n > 1$, the natural $M_n(\Delta)$ module structure on Δ^n (acting by linear transformations) is not free. Suppose it had a basis $\{x_i\}$. Take some basis element x_i; it is non-zero, i.e. it has some non-zero entry, call it x_{ij}. First, suppose that there is only one possible choice of j; in other words, x_i only has a non-zero entry in one spot. Let E_{ab} denote the matrix with 1 in (a, b) entry and 0 elsewhere. Then $E_{kk}x_i = 0$ for $k \neq j$, contradicting the fact that x_i is a basis element. Therefore, there are two indices j, j' for which $x_{ij}, x_{ij'} \neq 0$. Since $x_{ij}, x_{ij'}$ are elements of a division ring Δ, they have inverses. Thus $x_{ij}^{-1}E_{1j}x_i = x_{ij'}^{-1}E_{1j'}x_i$, i.e. $(x_{ij}^{-1}E_{1j} - x_{ij'}^{-1}E_{1j'})x_i = 0$, but $x_{ij}^{-1}E_{1j} - x_{ij'}^{-1}E_{1j'} \neq 0$, once again contradicting the assumption that x_i is a basis element. It follows that $M_n(\Delta)$ for $n > 1$ is not a ring satisfying the property that all modules are free. Therefore, our ring R, which does satisfy the property that all modules are free, and is also isomorphic to $M_n(\Delta)$ for some n, must be isomorphic to $M_1(\Delta)$, i.e. Δ. In particular, R is a division ring. □

2 Problem 18.2.12

Let F be a field, let $f(x) \in F[x]$ and let $R = F[x]/(f(x))$. Find necessary and sufficient conditions on the factorization of $f(x)$ in $F[x]$ so that R is a semisimple ring. When R is semisimple, describe its Wedderburn decomposition.

Proof. We will need to establish a preliminary result, namely that a direct product of commutative rings is semisimple if and only if each ring in the product is semisimple. This result requires another result, which requires another, and so on. Therefore, this proof will be somewhat lengthy and hard to follow. You may skip down to the paragraph starting with "Proposition 16 in section 9.5 ..." for the main proof, assuming this preliminary result.

First, we show that a commutative matrix ring over a division ring is a field. For this we apply part 2 of Proposition 6 in section 18.2 of Dummit and Foote, which in particular says that the center of a matrix ring over a division ring is a field. Since a commutative ring equals its center, this implies the result.

As an immediate corollary, Wedderburn's theorem applied to commutative rings says that a commutative ring is semisimple if and only if it is a product of fields.

We now show that a quotient of a semisimple commutative ring is semisimple. Let R be a semisimple commutative ring, and let J be an ideal. From above, we know that R is a direct product of fields. A basic fact in ring theory is that the ideals of a product of rings are precisely the products of ideals of each term in the product. Since fields only have two ideals, 0 and the whole field, this implies J is a product of 0 and fields appearing in the product decomposition of R. Then the quotient R/J is the product of fields which are in the decomposition of R but not in the decomposition of J, hence it is semisimple.

We now show that a product of a commutative ring with a non-semisimple commutative ring is non-semisimple ring. Let $R = A \times B$ be a ring where A, B are commutative rings and B is not semisimple. Let A' be the ideal of R consisting of $(a, 0) \in R = A \times B$. Clearly, $R/A' \cong B$, since any $(a, b) \in R$ is uniquely in the A' coset $(0, b) + A'$ for $b \in B$, and the multiplication checks out, and so on. We now have that a quotient of R is not semisimple, so R is not semisimple.

Finally, we show the desired preliminary result; a direct product of commutative rings is semisimple if and only if each ring in the product is semisimple. It is immediate from the last result that if any of the rings in the product is not semisimple, then the whole product is not semisimple. This gives one direction of the proof. For the other direction, we must show that a product of semisimple rings is semisimple. By Wedderburn's theorem, a ring is semisimple if and only if it has a direct product decomposition into matrix rings over division rings. Each term in the product is semisimple, so it admits a product decomposition

into matrix rings. This gives the whole product a product decomposition into matrix rings, so it is semisimple, as desired.
Proposition 16 in section 9.5 of Dummit and Foote gives a direct product decomposition for R in terms of the irreducible factorization of $f(x)$. Namely, if $f(x) = \prod_{i=1}^{k} f_i(x)^{n_i}$ where $f_i(x)$ is irreducible for $i = 1, ..., k$, then $R \cong \prod_{i=1}^{k} F[x]/(f_i(x)^{n_i})$. We will first analyze under what conditions on n a ring $F[x]/(p(x)^n)$ is semisimple for an irreducible polynomial $p(x)$.

If $n = 1$, then $R = F[x]/(p(x))$ is a field, namely $F(\alpha)$ where $p(\alpha) = 0$. In this case, R is a simple R-module, so R satisfies condition 4 of Wedderburn's theorem, so R is semisimple.

If $n > 1$, then we claim $R = F[x]/(p(x)^n)$ is not semisimple. Recall that the ideals of $F[x]/(p(x)^n)$ are in bijection with the ideals of $F[x]$ which contain $(p(x)^n)$ (this is a general result on ideals of quotient rings). Furthermore, $F[x]$ is a PID, so any ideal containing $(p(x)^n)$ is given by $(g(x))$ where $g(x)$ divides $p(x)^n$. Since $p(x)$ is irreducible, the only divisors of $p(x)^n$ (up to units, which do not matter for ideals) are powers of $p(x)$. Thus, in $R = F[x]/(p(x)^n)$, the only ideals are $0, (p(x)^{n-1}), ..., (p(x)), R$. In particular, $(p(x)^{n-1})$ is the only non-zero simple ideal, since we have the chain of containments $0 \subset (p(x)^{n-1}) \subset ... \subset (p(x)) \subset R$. If R were semisimple, Wedderburn's theorem says that there is a direct sum decomposition of R into simple principal ideals. As we have seen, there is only one such ideal in R, so there cannot be such a direct sum decomposition. Thus, R is not semisimple.

To summarize, we have proved that for irreducible $p(x)$, the ring $F[x]/(p(x)^n)$ is semisimple if and only if $n = 1$. Then, for an arbitrary polynomial $f(x)$, the ring $F[x]/(f(x))$ is a direct product of these rings. Together with the result proved in the first half of this solution, we can conclude that $F[x]/(f(x))$ is semisimple if and only if $f(x)$ is a product of distinct irreducibles, and the Wedderburn components are the fields $F[x]/(f_i(x))$ for each irreducible factor $f_i(x)$. □

3 Problem 18.2.13

Let G be the cyclic group of order n and let $R = \mathbb{Q}G$. Describe the Wedderburn decomposition of R and find the number and the degrees of the irreducible representations of G over $\mathbb{Q}$. In particular, show that if $n = p$ is a prime, then G has exactly one nontrivial irreducible representation over $\mathbb{Q}$ and this representation has degree $p - 1$.

Proof. From Section 18.1 of Dummit and Foote, we know that $\mathbb{Q}G = \mathbb{Q}[x]/(x^n - 1)$. From Proposition 9.5.16 of DF, and the fact that $x^n - 1 = \prod_{d|n} \Phi_d(x)$, we know that $\mathbb{Q}[x]/(x^n - 1) \cong \prod_{d|n} \mathbb{Q}[x]/(\Phi_d(x))$. Since each $\Phi_d(x)$ is irreducible, each $\mathbb{Q}[x]/(\Phi_d(x))$ is a field, and a field F is a ring of 1x1 matrices over itself. Then $\prod_{d|n} \mathbb{Q}[x]/(\Phi_d(x))$ is the Wedderburn decomposition of $\mathbb{Q}G$. The irreducible representations of G over $\mathbb{Q}$ are exactly the simple $\mathbb{Q}G$ modules, and by Proposition 18.2.8 of DF, we know that these are in bijection with the unique simple $\mathbb{Q}[x]/(\Phi_d(x))$ module for each $d \mid n$. Thus the number of irreducible representations of G over $\mathbb{Q}$ is exactly the number of (positive) divisors of n. Since $\mathbb{Q}[x]/(\Phi_d(x))$ is a field, a simple module over it is a one-dimensional vector space. As a $\mathbb{Q}$ vector space, it has dimension $[\mathbb{Q}[x]/(\Phi_d(x)) : \mathbb{Q}] = \deg \Phi_d(x) = \varphi(d)$. Thus the degree of the irreducible representation corresponding to $d \mid n$ is $\varphi(d)$. Applying these results to the case where $n = p$, we have two divisors and two irreducible representations of degree $\varphi(1) = 1$ and $\varphi(p) = p - 1$. □

4 Problem 18.2.17

Let F be a field, let $R = M_n(F)$, and let M be the unique irreducible R-module. Prove that $\text{Hom}_R(M, M)$ is ring-isomorphic to F.

Proof. By Proposition 6 in section 18.2 of Dummit and Foote, M can be realized as the (left) ideal of R consisting of n by n matrices with 0's in the $n - 1$ right-most columns. In fact another way of understanding this is that M is just the vector space F^n with R acting as F-linear transformations (with respect to the standard basis on F^n). Then $\text{Hom}_R(M, M)$ consists of linear transformations $F^n \to F^n$ which commute with the R-action on M. In otherwords, $\text{Hom}_R(M, M)$ is the center of R, which by Proposition 18.2.6 we know is a field isomorphic to the center of F, which is just F. $\square$

5 Problem 18.2.18

Find all 2-sided ideals of $M_n(\mathbb{Z})$.

Proof. Note: I will write "ideal" for "2-sided ideal".

We claim that all the ideals of $M_n(\mathbb{Z})$ are given by $M_n(J)$ for each ideal $J = (j)$ of $\mathbb{Z}$, where $M_n(J)$ means the set of n by n matrices with entries in J. By the definition of matrix multiplication and ideals, it is clear that each of these is an ideal, with $J = 0$ corresponding to the 0 ideal in $M_n(\mathbb{Z})$, and $J = \mathbb{Z}$ corresponding to the full ideal $M_n(\mathbb{Z})$.

Let I be a nonzero ideal in $M_n(\mathbb{Z})$. Let $J = \{x \in \mathbb{Z} \mid x = (A)_{ij} \text{ for some } A \in I \text{ and some } i, j\}$. We will show that J is an ideal in $\mathbb{Z}$, and that $I = M_n(J)$. First, notice that if $x = (A)_{ij}$ for $A \in I$, then we can find a matrix $B \in I$ such that $x = (B)_{1,1}$, as follows: Let E_{ij} be the matrix in $M_n(\mathbb{Z})$ with $(E_{ij})_{k\ell} = \delta_{ik}\delta_{j\ell}$. Then $E_{ij}AE_{k\ell} = (A)_{jk}E_{i\ell} \in I$. In particular, if $B = E_{1i}AE_{j1}$, then $(B)_{1,1} = (A)_{ij}$. As a result, we see that $J = \{x \in \mathbb{Z} \mid z = (A)_{1,1} \text{ for some } A \in I\}$, which is clearly an ideal; $(A + B)_{1,1} = (A)_{1,1} + (B)_{1,1}$ and $((rI)A)_{1,1} = r(A)_{1,1}$ for any $r \in \mathbb{Z}$.

We are left to prove $M_n(J) = I$. Clearly $I \subset M_n(J)$ by definition of J. Let $A \in M_n(J)$. We have $A = \sum_{i,j}(A)_{ij}E_{ij}$, and each $(A)_{ij} \in J$, so that $(A)_{ij} = (B)_{k\ell}$ for some $B \in I$ and some k, ℓ. But then $(A)_{ij}E_{ij} = (B)_{k\ell}E_{ij} = E_{ik}BE_{\ell j} \in I$, so that A is a sum of elements in I, so $A \in I$, as desired. □