Math 747 **Advanced Modern Algebra** Fall 2013

JERZY WOJCIECHOWSKI 12/06/2013 8:06am

Contents

1. Modules over Principal Ideal Domains.

Two Results in Algebra.

Structure of Finite Abelian Groups.

Theorem 1.1. *Let M be a finite abelian group (written additively). Then M is a direct product $\prod_{i=1}^{n} M_i$ of cyclic groups such that $\left|M_i\right| = p_i^{k_i}$ for some prime integers $p_1, \ldots, p_n$ and positive integers $k_1, \ldots, k_n$.*

Jordan Canonical Form of Matrices.

Theorem 1.2. *Let V be a finite dimensional vector space over $\mathbb{C}$ and $\varphi : V \to V$ be a linear function. Then there is a basis $v_{1,1}, \ldots, v_{1,k_1}, v_{2,1}, \ldots, v_{k_2}, \ldots, v_{n,1}, \ldots, v_{n,k_n}$ of V and $a_1, \ldots, a_n \in \mathbb{C}$ such that for every $i = 1, \ldots, n$ we have $\varphi\left(v_{i,t}\right) = a_i v_{i,t} + v_{i,t+1}$ when $t = 1, \ldots, k_i - 1$ and $\varphi\left(v_{i,k_i}\right) = a_i v_{i,k_i}$.*

Remark. Note that the matrix of φ with respect to the basis described in the theorem above has the form

$$\begin{matrix} A_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & A_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & A_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & A_{n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & A_n \end{matrix},$$

where A_j is the $k_j \times k_j$ matrix

$$\begin{matrix} a_j & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & a_j & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & a_j & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & a_j & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & a_j & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & a_j & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & a_j \end{matrix}$$

Connection between the Results.

The two results above are special cases of a theorem concerning finitely generated torsion modules over principal ideal domains. In the first result we specialize the theorem to modules over $\mathbb{Z}$ and in the second to modules over the $\mathbb{C}[x]$ (polynomials over $\mathbb{C}$). Recall that both $\mathbb{Z}$ and $\mathbb{C}[x]$ are principal ideal domains.

Modules over General Rings.

Rings.

Recall that a ring R has two operations, addition and multiplication, such that:

1. R is an abelian group under $+$.
2. Multiplication is associative and has the identity element $1 \in R$.
3. Addition is distributive (on both sides) with respect to multiplication.

Modules.

Let R be a ring. An R-module (a left R-module) is an abelian group M with a scalar multiplication $R \times M \to M$ such that:

1. $(a+b)m = am + bm$;
2. $a(m+n) = am + an$;
3. $(ab)m = a(bm)$;
4. $1m = m$;

for every $a, b \in R$ and $m, n \in M$, with 1 being the multiplicative identity of R.

Examples of Modules.

1. Let F be a field. Any vector space over F is an F-module.
2. Any abelian group M is a $\mathbb{Z}$-module with scalar multiplication defined by
$$km = \begin{cases} 0 & k = 0; \\ \underbrace{m + \cdots + m}_{k} & k > 0; \\ (-k)m & k < 0; \end{cases}$$
for any $k \in \mathbb{Z}$ and $m \in M$.
3. For any ring R and any positive integer n, the product
$$R^n = \underbrace{R \times \ldots \times R}_{n}$$
of n copies of R is an R-module with scalar multiplication being the componentwise multiplication in R.
4. Let R be a commutative ring and I be any ideal in R, then I is an R-module with scalar multiplication being the multiplication of R.
5. Let R be any ring. A left ideal in R is an additive subgroup S of R such that $rs \in S$ for any $r \in R$. Any left ideal of R is an R-module with scalar multiplication being the multiplication of R.

Homework 1 (due 8/21).

Let M be an abelian group (under $+$) and $\mathrm{End}(M)$ be the set of all homomorphisms $f : M \to M$. Define addition on $\mathrm{End}(M)$ by $\left(f+g\right)(m) = f(m) + g(m)$ and let multiplication be the composition.

1. Prove that $\mathrm{End}(M)$ is a ring.

2. Prove that any ring is a subring of $\mathrm{End}(M)$ for some M.

3. Let $f : R \to \mathrm{End}(M)$ be a ring homomorphism. Define scalar multiplication $R \times M \to M$ by $am = \big(f(a)\big)(m)$. Prove that M is an R-module.

Modules over Commutative Rings.

Assume that R is a commutative ring.

Torsion Modules.

Definition. An R-module M is torsion iff for every $m \in M$ there exists $r \in R \setminus \{0\}$ with $rm = 0$.

Example. Note that any finite abelian group is a torsion $\mathbb{Z}$-module. The quotient group $\mathbb{Q}/\mathbb{Z}$, which is infinite, is also a torsion $\mathbb{Z}$-module.

Finitely Generated Modules.

Definition. An R-module M is finitely generated iff there exist finitely many elements $a_1, \ldots, a_n \in M$ that generate M, that is, iff each $m \in M$ can be expressed as a linear combination $m = r_1 a_1 + \cdots + r_n a_n$ for some $r_1, \ldots, r_n \in R$.

Remark. Note that, trivially, any finite abelian group is a finitely generated $\mathbb{Z}$-module (take all the elements as generators). The infinite abelian group $\mathbb{Z}$ is also a finitely generated $\mathbb{Z}$-module. It is generated by one element $1 \in \mathbb{Z}$.

Proposition 1.3. *Let M be an abelian group. Then M is a finitely generated torsion $\mathbb{Z}$-module if and only if M is finite.*

Proof. Of course, any finite abelian group is a finitely generated torsion $\mathbb{Z}$-module. Assume that M is a finitely generated torsion $\mathbb{Z}$-module. Let $a_1, \ldots, a_n \in M$ generate M and for each $i = 1, \ldots, n$, let $k_i \in \mathbb{Z}$ be positive and such that $k_i a_i = 0$. Then each $m \in M$ can be expressed as

$$m = t_1 a_1 + \cdots + t_n a_n$$

with $t_i \in \left\{0, 1, \ldots, k_i - 1\right\}$. There are at most $k_1 k_2 \ldots k_n$ such linear combinations so M is finite. □

Homework 2 (due 8/23).

Prove that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module and that $\mathbb{Q}/\mathbb{Z}$ is not a finitely generated $\mathbb{Z}$-module without using Proposition 1.3.

Annihilator of a Module.

Definition. Let M be an R-module. The annihilator $\mathrm{ann}_R(M)$ is the set of all $r \in R$ so that $ra = 0$ for every $a \in M$. Note that $\mathrm{ann}_R(M)$ is an ideal in R.

Example. Consider the torsion $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$. Then $\mathrm{ann}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}) = \{0\}$. For the $\mathbb{Z}$-module $\mathbb{Z}_n$ we have $\mathrm{ann}_{\mathbb{Z}}\big(\mathbb{Z}_n\big) = n\mathbb{Z}$.

Proposition 1.4. *Let R be an integral domain and M be a finitely generated torsion R-module. Then there exists nonzero $r \in R$ such that $ra = 0$ for every $a \in M$. In particular, the annihilator $\mathrm{ann}_R(M)$ is a nonzero ideal of R.*

Proof. Let $a_1, \ldots, a_n \in M$ generate M over R. Since M is torsion, there are nonzero $r_1, \ldots, r_n \in R$ with $r_i a_i = 0$ for each $i = 1, \ldots, n$. Then $r = r_1 r_2 \ldots r_n \neq 0$ and $ra = 0$ for every $a \in M$. □

An Example of a Module over the Ring of Polynomials.

Definition. Let F be a field, V be a vector space over F and $R = F[x]$ be the ring of polynomials over F. If $\varphi : V \to V$ is a linear function, then we can make V to be an R-module with scalar multiplication defined as follows. If $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $v \in V$, then let the product fv be:

$$fv = a_0 v + a_1 \varphi(v) + a_2 \varphi^2(v) + \cdots + a_n \varphi^n(v),$$

where $\varphi^i = \underbrace{\varphi \circ \cdots \circ \varphi}_{i}$ is the composition of i copies of φ. We will denote such a module by V_φ.

Proposition 1.5. *Let R, S be commutative rings $f : R \to S$ be a ring homomorphism and $a \in S$ be a fixed element. Then there exists exactly one ring homomorphism $g : R[x] \to S$ that extends f and maps x to a.*

Corollary 1.6. *Let R be a commutative ring, S be any ring, $f : R \to S$ be a ring homomorphism and $a \in S$ be a fixed element that commutes with $f(r)$ for any $r \in R$. Then there exists exactly one ring homomorphism $R[x] \to S$ that extends f and maps x to a.*

Proof. Note that the subring S' of S generated by $f(R) \cup \{a\}$ is commutative. □

Remark. Let V be a vector space over a field F. Considering V as an abelian group, we have a ring homomorphism $f : F \to \mathrm{End}(V)$ mapping $a \in F$ to the endomorphism of V that is the scalar multiplication by a. If $\varphi : V \to V$ is a linear map, then $\varphi \in \mathrm{End}(V)$ and it commutes with $f(a)$ for any $a \in F$. Thus f can be extended to a unique ring homomorphism $F[x] \to \mathrm{End}(V)$ that maps x to φ. The structure of an $F[x]$-module on V_φ is then obtained as in point 3. of Homework 1.

Lemma 1.7. *If V is a finitely dimensional vector space over a field F, and $\varphi : V \to V$ is a linear function, then the $F[x]$-module V_φ as defined above is finitely generated and torsion.*

Proof. Since V is finitely dimensional over F, there is a finite basis of V over F. This basis obviously generates V_φ over $F[x]$. Thus V_φ is finitely generated.

Let n be the dimension of V. If $v \in V$, then $v, \varphi(v), \dots, \varphi^n(v)$ are linearly dependent so there are $a_0, a_1, \dots, a_n \in F$, not all zeros, with

$$a_0 v + a_1\varphi(v) + \cdots + a_n\varphi^n(v) = 0.$$

Then the polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ is nonzero and $f v = 0$. Thus V_φ is torsion. □

Cyclic Modules.

Definition. An R-module M is cyclic if it is generated by one element $a \in M$.

The Structure Theorem for Modules over PID.

Theorem 1.8. *Let R be a principal ideal domain and M be a finitely generated torsion R-module. Then M is isomorphic to a finite direct product $M = \prod_{i=1}^n M_i$ with each M_i being cyclic and $ann_R\big(M_i\big) = p_i^{k_i}R$ for some prime $p_i \in R$ and a positive integer k_i.*

Proof of Theorem 1.1.

Let M be a finite abelian group. Then M is a finitely generated torsion $\mathbb{Z}$-module so M is isomorphic to a finite direct product $\prod_{i=1}^n M_i$ of cyclic $\mathbb{Z}$-modules so that for each $i = 1, \dots, n$ we have $\operatorname{ann}_R\big(M_i\big) = p_i^{k_i}\mathbb{Z}$ for some prime $p_i \in \mathbb{Z}$ and a positive integer k_i. Clearly, we can chose every p_i to be positive. Then $\big|M_i\big| = p_i^{k_i}$ for each $i = 1, \dots, n$ and the proof is complete.

Submodules.

Definition. Let M be an R-module. A subset $N \subseteq M$ is a submodule of M if it is a subgroup under addition and is closed under scalar multiplication.

Remark. Consider a ring R as a module over itself. A subset $N \subseteq R$ is a submodule if and only if it is a left ideal of R.

Proposition 1.9. *Let M an R-module isomorphic to a direct product $\prod_{i=1}^n N_i$ of R-modules. Then for each $i = 1, \dots, n$ there exists a submodule M_i of M that is isomorphic to N_i and each $m \in M$ can be uniquely expresses as $m = m_1 + \cdots + m_n$ with $m_i \in M_i$ for each i.*

Homework 3 (due 8/28).

Let F be a field, k be a positive integer, $a \in F$ and $p(x) = x - a$. Prove that for any polynomial $f(x) \in F[x]$ there are $b_0, b_1, \dots, b_{k-1} \in F$ such that the polynomial

$$b_0 + b_1 p(x) + b_2 p(x)^2 + \cdots + b_{k-1} p(x)^{k-1} - f(x)$$

is divisible by $p(x)^k$.

Proof of Theorem 1.2.

Let V be a finite dimensional vector space over $\mathbb{C}$ and $\varphi : V \to V$ be a linear function. Then V_φ is a finitely generated torsion $\mathbb{C}[x]$-module so V_φ is isomorphic to finite direct product $\prod_{i=1}^n M_i$ of cyclic $\mathbb{C}[x]$-modules so that for each $i = 1, \dots, n$ we have $\mathrm{ann}_R(M_i) = p_i^{k_i}\mathbb{C}[x]$ for some prime $p_i \in \mathbb{C}[x]$ and a positive integer k_i. By Proposition 1.9, we can assume that $M_1, \dots, M_n$ are submodules of M and that each $m \in M$ can be uniquely expresses as $m = m_1 + \cdots + m_n$ with $m_i \in M_i$ for each i.

Since $\mathbb{C}$ is algebraically closed, the prime elements in $\mathbb{C}[x]$ are of first degree and we can choose each p_i to be of the form $x - a_i$ with $a_i \in \mathbb{C}$. For each $i = 1, \dots, n$, let $v_{i,1}$ be a generator of the module M_i and let $v_{i,j+1} = p_i v_{i,j}$ for every $j = 0, 1, \dots, k_i$. Then

$$v_{1,1}, \dots, v_{1,k_1}, v_{2,1}, \dots, v_{k_2}, \dots, v_{n,1}, \dots, v_{n,k_n}$$

is the required basis of V over F.

Remark. Theorem 1.2 (with the same proof) holds for any finitely dimensional vector space over an algebraically closed field F (instead of being over $\mathbb{C}$).

Homework 4 (due 9/9).

Let F be an arbitrary field, V be a finite dimensional vector space over F and $\varphi : V \to V$ be a linear function. Prove that there exists a basis of V with respect to which the matrix of φ will be of the form

$$\begin{matrix} A_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & A_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & A_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & A_{n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & A_n \end{matrix},$$

where A_i has the form

$$\begin{matrix} 0 & 0 & 0 & \cdots & 0 & 0 & a_{i,1} \\ 1 & 0 & 0 & \cdots & 0 & 0 & a_{i,2} \\ 0 & 1 & 0 & \cdots & 0 & 0 & a_{i,3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & a_{i,t_{i-2}} \\ 0 & 0 & 0 & \cdots & 1 & 0 & a_{i,t_{i-1}} \\ 0 & 0 & 0 & \cdots & 0 & 1 & a_{i,t_i} \end{matrix}$$

for some positive integer t_i and some $a_{i,1},\dots,a_{i,t_i} \in F$.

Proof of Theorem 1.8.

Annihilation by Prime Powers.

Definition. Let R be an integral domain and M be an R-module. For each prime $p \in R$, let $M(p)$ consist of all elements $a \in M$ such that there exists a positive integer k with $p^k a = 0$.

Remark. $M(p)$ is a submodule of M.

Example. If M is a $\mathbb{Z}$-module (abelian group) and p is a prime integer, then $M(p)$ consists of elements whose order is a power of p.

Prime Representatives.

Let R be an integral domain. Recall that $a, b \in R$ are associate iff $a = bu$ for some unit $u \in R$ and that the relation of being associate is an equivalence relation. For each class containing a prime fix one element of the class. We will call those fixed elements the prime representatives in R.

Lemma 1.10. *Let M be a nontrivial finitely generated torsion module over a principal ideal domain R. There exists a finite set I of prime representatives in R with $M(p) \neq \{0\}$ for each $p \in I$ and*

$$M \cong \prod_{p \in I} M(p).$$

Proof. Let $a \in R$ be nonzero with $am = 0$ for every $m \in M$. Let $a = up_1^{r_1} \dots p_n^{r_n}$, where u is a unit, $p_1,\dots,p_n$ are distinct prime representatives in R and $r_1,\dots,r_n$ are positive integers. Let $M' = \prod_{i=1}^n M(p_i)$ and $\varphi : M' \to M$ be defined by $\varphi(t_1,\dots,t_n) = t_1 + \dots + t_n$. Clearly φ is a homomorphism. Let $(t_1,\dots,t_n) \in \ker(\varphi)$. For each $i = 1,\dots,n$, let k_i be a positive integer such that $p_i^{k_i} t_i = 0$. Let $q, s \in R$ be such that $1 = qp_1^{k_1} + sp_2^{k_2} \dots p_n^{k_n}$. Then $t_1 = -(t_2 + \dots + t_n)$ so

$$\begin{aligned} t_1 &= \left(qp_1^{k_1} + sp_2^{k_2} \dots p_n^{k_n}\right) t_1 \\ &= qp_1^{k_1} t_1 + sp_2^{k_2} \dots p_n^{k_n} t_1 \\ &= -sp_2^{k_2} \dots p_n^{k_n} (t_2 + \dots + t_n) \\ &= 0. \end{aligned}$$

Similarly, $t_i = 0$ for each $i = 2,\dots,n$. Thus φ is injective.

Let $m \in M$ be arbitrary. For each $i = 1,\dots,n$, let $q_i \in R$ be such that

$$1 = \sum_{i=1}^n q_i \prod_{j \in \{1,\dots,n\} \setminus \{i\}} p_j^{r_j},$$

and

$$m_i = \left(q_i \prod_{j \in \{1,\ldots,n\} \setminus \{i\}} p_j^{r_j} \right) m \in M_i.$$

Then $m = \varphi(m_1, \ldots, m_n)$ so φ is surjective. □

Submodules of Finitely Generated Modules.

Lemma 1.11. *Let M be a finitely generated module over a principal ideal domain. Then every submodule N of M is also finitely generated.*

Proof. Let $a_1, \ldots, a_n$ generate M. We will show that there exist $b_1, \ldots, b_n \in N$ that generate N. The proof is by induction on n. We show that there exists $b_1 \in N$ such that the submodule of M generated by $b_1, a_2, a_3, \ldots, a_n$ contains N. Then we apply the inductive hypothesis to the submodule M' of M generated by $a_2, \ldots, a_n$ and its submodule $N' = M \cap N$ obtaining $b_2, \ldots, b_n \in N'$ that generate N'. Now each element $a \in N$ is of the form $\gamma b_1 + b$ with $\gamma \in R$ and $b \in N'$. So $b_1, \ldots, b_n$ generate N.

To show the existence of the required $b_1 \in N$, let I be the set consisting of all $r \in R$ so that some element of N is of the form $ra_1 + c$ with c being a linear combination of $a_2, \ldots, a_n$. Then I is an ideal of R. Let $s \in I$ be such that $I = sR$. Then some element $b_1 \in N$ is of the form $b_1 = sa_1 + c$ with c being a linear combination of $a_2, \ldots, a_n$. □

Remark. Let F be a field, X be an infinite set of variables and $R = F[X]$ be the ring of all polynomials with coefficients in F. Then R is a finitely generated R-module (cyclic) but the submodule M of R consisting of those polynomials whose constant term is equal to 0 is not finitely generated. The ring R is a unique factorization domain, so the lemma is not true when we replace principal ideal domains with unique factorization domains.

Quotient Modules.

Let M be an R-module and N be a submodule of M. The quotient module M/N is the quotient abelian group with scalar multiplication defined by $a(b+N) = ab + N$ for any $a \in R$ and $b \in M$. If $b + N = b' + N$, then $b - b' \in N$ so $a(b - b') = ab - ab' \in N$ implying that $ab + N = ab' + N$. Thus the scalar multiplication is well-defined. It is routine to verificar that M/N is an R-module under this identification.

Correspondence Theorem for Modules.

Let M be an R-module and N be a submodule of M. Any submodule of M/N is of the form M'/N for some submodule M' of M containing N. The proof is routine.

Direct Sum of Submodules.

Let M be an R-module and $M_1, \ldots, M_n$ be submodules of M. The sum $M' = \sum_{i=1}^{n} M_i$ is the set of elements of the form $a_1 + \cdots + a_n$ with $a_i \in M_i$ for each i. Clearly M' is a submodule of M. We say that the sum is direct if such an expression is unique for each $m \in M'$ and we write then $M = \bigoplus_{i=1}^n M_i$.

Remark. Let M be an R-module and $M_1, \ldots, M_n$ be submodules of M. Then $M = \bigoplus_{i=1}^n M_i$ if and only if $\varphi : \prod_{i=1}^n M_i \to M$ given by $\varphi(a_1, \ldots, a_n) = a_1 + \cdots + a_n$ is an isomorphism. Thus to verificar that $M = \bigoplus_{i=1}^n M_i$ it suffices to verificar that $M = \sum_{i=1}^n M_i$ and that if $a_1 + \cdots + a_n = 0$ with $a_i \in M_i$ for each i, then $a_i = 0$ for each i.

Modules Annihilated by Prime Powers.

Lemma 1.12. *Let R be a principal ideal domain, M be a finitely generated R-module, k be a positive integer and $p \in R$ be a prime such that $p^k m = 0$ for each $m \in M$. Then M is isomorphic to $\prod_{i=1}^n M_i$ with each M_i being cyclic.*

Proof. Let $m_1, \ldots, m_n$ generate M. We use induction on n to show that there are cyclic submodules $M_1, \ldots, M_n$ of M such that $M = \bigoplus_{i=1}^n M_i$.

If $n = 1$ then M is cyclic so there is nothing to prove. Assume that $n \geq 2$. For each $i = 1, 2, \ldots, n$ let k_i be the smallest nonnegative integer with $p^{k_i} m_i = 0$. We can assume without loss of generality that $k_1 = \max\{k_1, \ldots, k_n\}$ as otherwise we can permute the generators $m_1, \ldots, m_n$. Let $M_1 = Rm_1$ be the cyclic submodule of M generated by m_1.

(*) Let N be a submodule of M containing M_1 such that N/M_1 is cyclic. Then there exists $a \in N$ such that N/M_1 is generated by $a + M_1$ and $\operatorname{ann}_R(a) = \operatorname{ann}_R(a + M_1)$.

Proof of (*). Let $b \in N$ be any element such that $b+M_1$ generates N/M_1. Let $\operatorname{ann}_R(b) = p^t R$. Then $\operatorname{ann}_R(b + M_1) = p^s R$ for some $s \leq t$ and consequently $p^s b \in M_1$. Since m_1 generates M_1, we have $p^s b = q m_1$ for some $q \in R$. Let $q = p^w v$ where w is a nonnegative integer and $v \in R$ is not divisible by p. Thus $p^s b = p^w v m_1$. Note that $v m_1$ is also a generator of M_1 so $\operatorname{ann}_R(v m_1) = p^{k_1} R$. Note also that

$$p^{k_1 - w} R = \operatorname{ann}_R(p^w v m_1) = \operatorname{ann}_R(p^s b) = p^{t-s} R.$$

Thus $k_1 - w = t - s$. Since $t \leq k_1$, it follows that $s \leq w$. Thus $p^s b = p^s c$ for $c = p^{w-s} v m_1 \in M_1$. Let $a = b - c$. Then $a + M_1 = b + M_1$ and $p^s a = 0$ implying that $\operatorname{ann}_R(a) = \operatorname{ann}_R(a + M_1)$. □

The quotient module M/M_1 is generated by $n-1$ elements $\overline{m_2}, \ldots, \overline{m_n}$, where $\overline{m_i} = m_i + M_1$, so by the inductive hypothesis

$$M/M_1 = \bigoplus_{i=2}^{n} M_i'/M_1$$

for some submodules $M_2', \ldots, M_n'$ of M containing M_1 such that each M_i'/M_1 is cyclic. By (*), we can select $m_2', \ldots, m_n'$ so that $\overline{m_i'}$ generates M_i'/M_1 and

$$\operatorname{ann}_R(m_i') = \operatorname{ann}_R(\overline{m_i'})$$

for each $i = 2, \ldots, n$. Let M_i be the cyclic submodule of M generated by m_i' for each $i = 2, \ldots, n$.

First we show that $M = \sum_{i=1}^n M_i$. Let $m \in M$. Then

$$\overline{m} = r_2 \overline{m_2'} + \cdots + r_n \overline{m_n'} = \overline{r_2 m_2' + \cdots + r_n m_n'}$$

for some $r_2, \ldots, r_n \in R$. Thus

$$m - \left(r_2 m_2' + \cdots + r_n m_n'\right) \in M_1$$

implying that $M = \sum_{i=1}^n M_i$.

Let $a_i \in M_i$ be such that $a_1 + \cdots + a_n = 0$. Note that the choice of m_i' implies that to prove that $a_i = 0$ for $i = 2, \ldots, n$, it suffices to show that $\overline{a_i} = 0$. Since

$$a_2 + \cdots + a_n = -a_1 \in M_1$$

it follows that $\overline{a_2} + \cdots + \overline{a_n} = 0$ in the quotient module M/M_1. Thus each $\overline{a_i}$ equals 0 for each i. Consequently $a_2 = a_3 = \cdots = a_n = 0$ which implies that $a_1 = 0$ as well. □

The Completion of the Proof of Theorem 1.8

Let R be a principal ideal domain and M be a finitely generated torsion R-module. By Lemma 1.10 there exists a finite set I of prime representatives in R with $M(p) \neq \{0\}$ for each $p \in I$ and

$$M \cong \prod_{p \in I} M(p).$$

Each $M(p)$ is finitely generated and there is a positive integer k_p such that $p^{k_p} m = 0$ for each $m \in M$. Thus each $M(p)$ is isomorphic to $\prod_{i=1}^{n_p} M_{p,i}$ with each $M_{i,p}$ being cyclic and $\mathrm{ann}_R\left(M_{p,i}\right) = p^{k_i} R$ for some positive integer $k_i \leq k_p$.

2. Group Representations and Modules over Group Rings.

Burnside Theorem.

Solvable Groups.

Definition. A group G is solvable iff there exists a chain of groups

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \left\{1_G\right\}$$

such that for each $i = 1, \ldots, n$, the group G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is abelian.

Remark. Let F be a field of characteristic zero, f be a polynomial over F and K be the splitting field of f over F. Recall that the following conditions are equivalent.

1. The polynomial f is solvable by radicals over F.

2. The Galois group of K over F is solvable.

Recall that the group A_5 consisting of all even permutations of five elements is not solvable. Note that the order of A_5 is $60 = 2^2 \cdot 3 \cdot 5$.

Also recall that if G is a group and H is a normal subgroup of G then the following conditions are equivalent:

1. G is solvable.

2. Both H and G/H are solvable.

Theorem 2.1 (Burnside). *Let p, q be primes and a, b be nonnegative integers. Any finite group of order $p^a q^b$ is solvable.*

Remark. The proof of Burnside Theorem uses the following lemma. Its proof will be presented later. It is based on group representations. There is a proof that does not use group representations but it is more complicated.

Lemma 2.2. *Let G be a finite non-abelian simple group. No conjugacy class of G has order p^a with p being a prime integer and a being a positive integer.*

Example. In the nonabelian group S_3 the conjugacy classes have orders 1, 2 and 3, however S_3 is not simple. In the simple nonabelian group A_5 the conjugacy classes have orders 1, 20, 15, 12, 12.

Homework 5 (due 9/11).

Prove that the conjugacy classes of A_5 have orders 1, 20, 15, 12, 12.

Proof of Burnside Theorem.

Let G be a group of order $p^a q^b$ with p, q being prime and a, b being nonnegative integers. Suppose, by way of contradiction, that G is not solvable and that G is of the smallest possible cardinality. Then G must be simple and non-abelian since, otherwise, if H were a nontrivial proper normal subgroup of G then either H or G/H would be non-solvable and would have smaller order than G. It follows that both a and b are positive (a group of prime power order is either cyclic or has a nontrivial center which is a normal subgroup).

Let P be a Sylow p-subgroup of G. Then the center Z of P is nontrivial. Let $z \in Z$ be a non-identity element. The centralizer $C(z)$ of z contains P so the index $[G : C(z)]$ is a power of q. Since $[G : C(z)]$ is equal to the order of the conjugacy class containing z it follows from Lemma 2.2 that $C(z) = G$. Thus z is in the center of G implying that the center of G is nontrivial. Since the center of G is a normal subgroup of G we have a contradiction.

Group Representations.

Definition. Let G be a group and R be a commutative ring. A representation of G over R is a group homomorphism $G \to \mathrm{Aut}_R(M)$ for some R-module M. Here $\mathrm{Aut}_R(M)$ is the group of all isomorphisms $M \to M$.

We will be mostly interested in the case when R is a field and especially the case when G is finite, $R = \mathbb{C}$ and M is finitely dimensional.

Faithful Representations.

Definition. We say that a group representation $\varphi : G \to \mathrm{Aut}_R(M)$ is faithful iff the the homomorphism φ is injective.

Proposition 2.3. *For every group there exists a faithful representation over any nontrivial commutative ring.*

Proof. Every group is isomorphic to a permutation group (a subgroup of all permutations of some set). Let R be a nontrivial commutative ring and A be a set. Then the set M of all functions $A \to R$ is an R-module. If $S(A)$ is the group of all permutations of A, then there exists an injective group homomorphism $S(A) \to \mathrm{Aut}_R(M)$. □

Homework 6 (due 9/13).

Define an injective group homomorphism $S(A) \to \mathrm{Aut}_R(M)$ for the proof of Proposition 2.3.

Monoid Rings and Group Rings.

Monoids.

Definition. A monoid is a set with a binary operation that is associative and has the identity element.

Example. Any group is a monoid. The nonnegative integers form a monoid under addition. Any ring under multiplication is a monoid.

Monoid Rings.

Definition. Let G be a monoid with the operation denoted as multiplication and R be a commutative ring. Let $R[G]$ be the set of all functions $\alpha : G \to R$ such that $\alpha\big(g\big) = 0$ for all but finitely many elements of $g \in G$. We define addition on $R[G]$ as $\big(\alpha + \beta\big)\big(g\big) = \alpha\big(g\big) + \beta\big(g\big)$ and multiplication by

$$\alpha\beta\big(g\big) = \sum_{ab=g} \alpha(a)\beta(b),$$

where the summation is taken over all pairs $(a, b) \in G \times G$ with $ab = g$. The sum is finite since there are only finitely many such pairs with $\alpha(a)$ and $\beta(b)$ being nonzero and since all the other pairs can be ignored.

Notation. An element $\alpha \in R[G]$ will be denoted as a sum $r_1 g_1 + r_2 g_2 + \cdots + r_n g_n$ where $\alpha(g_i) = r_i$ for all $i = 1, 2, \ldots, n$ and $\alpha(g) = 0$ for any $g \in G \setminus \{g_1, \ldots, g_n\}$. Note that using this notation, we have

$$\left(r_1 g_1 + \cdots + r_n g_n\right)\left(s_1 h_1 + \cdots + s_m h_m\right) = \sum_{i=1}^{n} \sum_{j=1}^{m} r_i s_j \left(g_i h_j\right).$$

Example. Let R be a commutative ring. The monoid ring $R[\mathbb{N}]$ is isomorphic to the ring $R[x]$ of polynomials in one variable. The isomorphism maps the polynomial $r_0 + r_1 x + r_2 x^2 + \cdots + r_n x^n$ to $\alpha \in R[\mathbb{N}]$ with $\alpha(i) = r_i$ for $i = 0, 1, \ldots, n$ and $\alpha(i) = 0$ for $i > n$.

Group Rings.

A group ring is a monoid ring with the monoid being a group.

Remark. Given a group ring $R[G]$, we can identify an element $r \in R$ with the element $r 1_G \in R[G]$ and an element $g \in G$ with the element $1_R g \in R[G]$. Thus we may think of R and G as being subsets of $R[G]$. Moreover R becomes a subring of $R[G]$ and G becomes a submonoid of the multiplicative monoid of $R[G]$.

Modules over Group Rings.

Proposition 2.4. *Let M be an $R[G]$-module. If $\varphi : R[G] \to End(M)$ is the corresponding ring homomorphism, then the restriction of φ to G is a representation of G over R.*

Proof. Identifying the elements of R with the corresponding elements of $R[G]$, the and restricting the scalar multiplication to $R \times M$, we obtain an R-module M. Since φ assigns to an element $\beta \in R[G]$ the scalar multiplication by β and since β commutes with any element of R the resulting endomorphism $\varphi(\beta)$ of the the abelian group M preserves scalar multiplication by elements of R so $\varphi(\beta) \in \mathrm{End}_R(M)$. Every element of G is invertible in $R[G]$, so the restriction of φ to G is a group homomorphism $G \to \mathrm{Aut}_R(M)$. □

Remark. We see that any $R[G]$-module induces a representation of G over R.

Proposition 2.5. *Let G be a group and R be a commutative ring. If $\varphi : G \to Aut_R(M)$ is a representation of G, then φ can be extended uniquely to a ring homomorphism $R[G] \to End_R(M)$.*

Proof. Let $\psi : R[G] \to \mathrm{End}_R(M)$ be defined by

$$\left(\psi\left(r_1 g_1 + \cdots + r_n g_n\right)\right)(m) = r_1 \left(\varphi\left(g_1\right)(m)\right) + \cdots + r_n \left(\varphi\left(g_n\right)(m)\right)$$

for any $r_1, \ldots, r_n \in R$, any $g_1, \ldots, g_n \in G$ and any $m \in M$. For any $g \in G$, the image $\varphi(g)$ is in $\mathrm{Aut}_R(M)$ so it preserves the operation of addition of M and the scalar multiplication of the elements of M by the elements of R. Thus

$$\begin{aligned}
&\left(\psi(r_1g_1+\cdots+r_ng_n)\right)(m_1+m_2)\\
= \;& r_1\left(\varphi(g_1)(m_1+m_2)\right)+\cdots+r_n\left(\varphi(g_n)(m_1+m_2)\right)\\
= \;& r_1\left(\varphi(g_1)(m_1)+\varphi(g_1)(m_2)\right)+\cdots+r_n\left(\varphi(g_n)(m_1)+\varphi(g_n)(m_2)\right)\\
= \;& r_1\left(\varphi(g_1)(m_1)\right)+r_1\left(\varphi(g_1)(m_2)\right)+\cdots+r_n\left(\varphi(g_n)(m_1)\right)+r_n\left(\varphi(g_n)(m_2)\right)\\
= \;& \left(r_1\left(\varphi(g_1)(m_1)\right)+\cdots+r_n\left(\varphi(g_n)(m_1)\right)\right)+\left(r_1\left(\varphi(g_1)(m_2)\right)+\cdots+r_n\left(\varphi(g_n)(m_2)\right)\right)\\
= \;& \left(\psi(r_1g_1+\cdots+r_ng_n)\right)(m_1)+\left(\psi(r_1g_1+\cdots+r_ng_n)\right)(m_2),
\end{aligned}$$

so $\psi(r_1g_1+\cdots+r_ng_n)$ preserves addition, and

$$\begin{aligned}
\left(\psi(r_1g_1+\cdots+r_ng_n)\right)(rm) &= r_1\left(\varphi(g_1)(rm)\right)+\cdots+r_n\left(\varphi(g_n)(rm)\right)\\
&= r_1r\left(\varphi(g_1)(m)\right)+\cdots+r_nr\left(\varphi(g_n)(m)\right)\\
&= r\left(r_1\left(\varphi(g_1)(m)\right)+\cdots+r_n\left(\varphi(g_n)(m)\right)\right)\\
&= r\left(\psi(r_1g_1+\cdots+r_ng_n)(m)\right),
\end{aligned}$$

so $\psi(r_1g_1+\cdots+r_ng_n)$ preserves scalar multiplication. Thus the values of ψ are in $\mathrm{End}_R(M)$. It remains to verify that ψ is a ring homomorphism. It is clear that ψ preserves addition. We have also

$$\begin{aligned}
\left(\psi\left(\left(\sum_{i=1}^n r_ig_i\right)\left(\sum_{j=1}^k s_jh_j\right)\right)\right)(m) &= \psi\left(\sum_{i=1}^n\sum_{j=1}^k r_is_j\left(g_ih_j\right)\right)(m)\\
&= \sum_{i=1}^n\sum_{j=1}^k r_is_j\left(\varphi(g_ih_j)(m)\right)\\
&= \sum_{i=1}^n\sum_{j=1}^k r_is_j\left(\varphi(g_i)(\varphi(h_j)(m))\right)\\
&= \sum_{i=1}^n r_i\left(\varphi(g_i)\left(\sum_{j=1}^k s_j\left(\varphi(h_j)(m)\right)\right)\right)\\
&= \left(\psi\left(\sum_{i=1}^n r_ig_i\right)\right)\left(\psi\left(\sum_{j=1}^k s_jh_j\right)(m)\right)
\end{aligned}$$

for each $m \in M$, implying that

$$\psi\left(\left(\sum_{i=1}^n r_ig_i\right)\left(\sum_{j=1}^k s_jh_j\right)\right)=\psi\left(\sum_{i=1}^n r_ig_i\right)\circ\psi\left(\sum_{j=1}^k s_jh_j\right)$$

so ψ preserves multiplication. □

Remark. Propositions 2.4 and 2.5 show that defining a representation of a group G over a commutative ring R is equivalent to defining an $R[G]$-module.

Simple and Semisimple Modules.

Simple Modules.

Remark. To prove Lemma 2.2, we will be interested in representations of finite groups over $\mathbb{C}$. We will show that any such representation can be obtained from a finite collection of irreducible representations (when the corresponding $\mathbb{C}[G]$-module is simple). We will develop the theory of characters of representations that will be functions $G \to \mathbb{C}$. We will introduce a hermitian product on the vector space $\mathbb{C}^G$ and show that the characters of irreducible representations are orthonormal in that product.

Definition. An R-module M is simple iff M is nontrivial and does not have any nontrivial proper submodules.

Remark. A module over a field is simple iff it is one-dimensional as a vector space. The $\mathbb{Z}$-module $\mathbb{Z}$ is not simple simple since say $2\mathbb{Z}$ is a nontrivial proper submodule. A $\mathbb{Z}$-module M is simple iff M is a finite abelian group of prime order.

Schur's Lemma.

Proposition 2.6. *Let M and N be simple R-modules. If $\varphi : M \to N$ is a nonzero homomorphism, then it is an isomorphism.*

Proof. The kernel of φ is a submodule of M. Since it is not M, so it must be $\{0\}$. Thus φ is injective. The image of φ is a submodule of N. Since it is not $\{0\}$, it must be N. Thus φ is surjective. $\square$

Remark. If M is a simple R-module, then it follows that the ring $\mathrm{End}_R(M)$ is a division ring (every nonzero element has an inverse) since every nonzero element is an R-module isomorphism $M \to M$.

Sum and Direct Sum of Submodules.

Definition. Let M be a module and $\{M_i : i \in I\}$ be a (possibly infinite) family of submodules. The sum $\sum_{i\in I} M_i$ is the submodule M' of M consisting all sums $\sum_{i\in I} m_i$ with $m_i \in M_i$ for each $i \in I$ with all but finitely many of m_i being equal to zero.

The sum is direct iff the equality $0_M = \sum_{i\in I} m_i$ with $m_i \in M_i$ for every $i \in I$ implies that every m_i are equal to 0_{M_i}. The direct sum is denoted $\bigoplus_{i\in I} M_i$.

Lemma 2.7. *Let M be an R-module and $\varphi : M \to M$ be an R-homomorphism such that $\varphi^2 = \varphi$ (φ is identity on its image). Then $M = \mathrm{im}(\varphi) \oplus \ker(\varphi)$.*

Proof. Let $m \in M$. Then

$$\varphi\big(m - \varphi(m)\big) = \varphi(m) - \varphi^2(m) = 0,$$

so $m - \varphi(m) \in \ker(\varphi)$ implying that M is the sum of $\mathrm{im}(\varphi)$ and $\ker(\varphi)$. It remains to show that the sum is direct.

Suppose that $\varphi(m)+m'=0$ with $\varphi\big(m'\big)=0$. Then

$$0=\varphi\big(\varphi(m)+m'\big)=\varphi^2(m)+\varphi\big(m'\big)=\varphi(m),$$

and consequently also $m'=0$. Thus the sum is direct. $\square$

Semisimple Modules.

Theorem 2.8. *Let M be an R-module. The following conditions are equivalent.*

1. *M is a sum of simple submodules.*
2. *M is a direct sum of simple submodules.*
3. *For every submodule N of M there exists a submodule N' of M with $M=N\oplus N'$ (every submodule of M is a direct summand).*

Definition. An R-module M is semisimple iff it satisfies the conditions of Theorem 2.8.

Remark. Note that 3. is equivalent to:

3'. For every submodule N of M there exists an R-homomorphism $\varphi: M\to M$ such that $\varphi^2=\varphi$ and $\operatorname{im}\big(\varphi\big)=N$.

Proof. 3'. $\Rightarrow$ 3. By Lemma 2.7 we have $M=N\oplus\ker\big(\varphi\big)$.

3. $\Rightarrow$ 3'. Take a submodule N' of M such that $M=N\oplus N'$ and define $\varphi: M\to M$ by $\varphi(m)=n$ where $m=n+n'$ with $n\in N$ and $n'\in N'$. It remains to show that φ is well-defined and satisfies the required conditions. $\square$

Homework 7 (due 9/27).

Finish the proof that 3. $\Rightarrow$ 3'. in the remark above.

Proof of Theorem 2.8.

1. $\Rightarrow$ 2. Suppose the $M=\sum_{i\in I}M_i$ with each M_i being a simple submodule of M. Using Zorn's Lemma we show that there exists a maximal subset $J\subseteq I$ with the sum $M'=\sum_{i\in J}M_i$ being a direct sum. For each $i\in I$ the intersection $M_i\cap M'$ is a submodule of M_i so it is either equal to M_i or is trivial. However, if it were trivial it would contradict the maximality of J. It follows that any M_i is a submodule of M' implying that $M'=M$. Thus $M=\bigoplus_{i\in J}M_i$.

2. $\Rightarrow$ 3. Let $J\subseteq I$ be a maximal subset such that the sum $N+\sum_{i\in J}M_i$ is a direct sum. Arguing as above, we show that this sum equals M. Let $N'=\sum_{i\in J}M_i$.

3. $\Rightarrow$ **1.** Let $\{M_i : i \in I\}$ be the set of all simple submodules of M. It remains to show that $\sum_{i\in I} M_i = M$. Note that it suffices to show that every nonzero submodule of M contains a simple submodule. Then for $N = \sum_{i\in I} M_i$ we must have $N = M$ since otherwise there would be a submodule $N' \neq \{0\}$ of M with $M = N \oplus N'$ so N' would contain no simple submodules producing a contradiction.

Let N be any nonzero submodule of M and N'' be a maximal submodule of N. The existence of N'' can be proved using Zorn's Lemma. There exists a submodule N' of M such that $M = N'' \oplus N'$. Then $N = N'' \oplus (N' \cap N)$ and since N'' is a maximal submodule of N, it follows that $N' \cap N$ is a simple submodule of N.

Submodules and Quotient Modules of Semisimple Modules.

Remark. The first isomorphism theorem holds for R-modules. That is, for any R-homomorphism $\varphi : M \to N$ the image of φ is R-isomorphic to $\ker(\varphi)$. It follows that if M is an R-module and $M = N \oplus N'$ for some submodules N and N' of M, then N' is isomorphic to the quotient module M/N.

Proof. Let $\varphi : M \to N'$ be defined by $\varphi(m) = n'$ iff $m = n + n'$ for some $n \in N$ and $n' \in N'$. Then φ is a homomorphism of R-modules with $N = \ker(\varphi)$. Thus N' is isomorphic to M/N. □

Theorem 2.9. *Every submodule and every quotient module of a semisimple module is semisimple.*

Proof. Let M be a semisimple R-module and N be a submodule of M. Let $\{M_i : i \in I\}$ be the family of all simple submodules of M, let $J = \{i \in I : M_i \subseteq N\}$ and $N' = \sum_{i\in J} M_i$. Then $M = N' \oplus N''$ for some submodule N'' of M. Every element $n \in N$ is uniquely expressible as $n = n' + n''$ with $n' \in N'$ and $n'' \in N''$. Since $N' \subseteq N$, we have $n'' \in N'' \cap N$. Thus $N = N' \oplus (N'' \cap N)$. If $N'' \cap N$ were nontrivial, it would contain M_i for some $i \in I \setminus J$, a contradiction. Thus $N'' \cap N$ is trivial and $N = N'$ is semisimple.

Then M/N is isomorphic to N'' so it is also semisimple. □

Free Modules.

Linear Independence in Modules.

Definition. Let M be an R-module and $B \subseteq M$. We say that the set B is linearly independent iff for a positive integer n, for any distinct $b_1, \ldots, b_n \in B$ and for any $r_1, \ldots, r_n \in R$ the equality $r_1 b_1 + \cdots + r_n b_n = 0$ implies that $r_1 = \cdots = r_n = 0$.

Remark. The empty set is linearly independent in any R-module.

Basis of a Module.

Definition. Let M be an R-module. A basis of M is a subset of M that generates (spans) M and is linearly independent.

Remark. The empty set is a basis of the trivial R-module. If I is a proper nontrivial ideal of a ring R, then the quotient R-module R/I has no basis since any nonempty subset of R/I is linearly dependent (if $a \in I \setminus \{0\}$, then $a(r+I) = I$ equals zero in R/I for any $r \in R$).

Free Modules.

Definition. An R-module M is free iff it has a basis.

Lemma 2.10. *An R-module M is free if and only if $M = \bigoplus_{i\in I} M_i$ for some set I with each M_i isomorphic to R as a module over R.*

Proof. Assume that M is free and let $B = \left\{b_i : i \in I\right\}$ be a basis of M. Then $M = \bigoplus_{i\in I} M_i$ where $M_i = Rb_i$ for each $i \in I$. The map $\varphi_i : R \to M_i$ given by $\varphi_i(r) = rb_i$ is an R-isomorphism. Indeed, φ_i is an R-homomorphism since it clearly preserves addition and

$$\varphi_i(rs) = (rs)\, b_i = r\left(sb_i\right) = r\left(\varphi_i(s)\right).$$

It is clearly surjective and is injective since the singleton $\left\{b_i\right\}$ is linearly independent.

Suppose that $M = \bigoplus_{i\in I} M_i$ for some set I with each M_i isomorphic to R as a module over R. Let $\varphi_i : R \to M_i$ be an R-isomorphism. Then $B = \left\{\varphi_i\left(1_R\right) : i \in I\right\}$ is a basis of M. □

Definition. When $M = \bigoplus_{i\in I} M_i$ for some set I with each M_i isomorphic to R as a module over R, then we say that M is free over I.

Remark. An R-module M is free over I iff there exists a basis $B = \left\{b_i : i \in I\right\}$ of M.

Lemma 2.11. *For every set I there exists an R-module that is free over I.*

Proof. Let M be the set of all functions $f : I \to R$ such that $\left\{i \in I : f(i) \neq 0\right\}$ is finite. □

Homework 8 (due 10/2).

Let V be a vector space over $\mathbb{R}$ with a countable basis $\left\{x_0, x_1, \ldots\right\}$. For example, you can take $V = \mathbb{R}[x]$ and $x_i = x^i$ for each $i = 0, 1, \ldots$. Let $R = \mathrm{End}_{\mathbb{R}}(V)$ and consider R as a module over itself. Let

$$M_1 = \left\{\varphi \in R : \varphi\left(x_{2i}\right) = 0, \quad i = 0, 1, \ldots\right\}$$

and

$$M_2 = \left\{\varphi \in R : \varphi\left(x_{2i+1}\right) = 0, \quad i = 0, 1, \ldots\right\}.$$

Prove that both M_1 and M_2 are submodules of R that are isomorphic to R as R-modules and that $R = M_1 \oplus M_2$.

Remark. If $m_1 \in M_1$ and $m_2 \in M_2$ correspond to 1_R under the isomorphisms $R \to M_1$ and $R \to M_2$, then $\left\{m_1, m_2\right\}$ is a basis of R as an R-module. The set $\left\{1_R\right\}$ is also a basis of R. Using induction, for any positive integer n, we can obtain a basis of R as an R-module that consists of n elements.

The Invariant Dimension Property.

Definition. Let R be a ring. We say that R has the invariant dimension property if for every free R-module M, any two bases of M have the same cardinality.

Infinite Dimension is Always Invariant.

Lemma 2.12. *Let R be any ring and M be a free R-module with an infinite basis B. Then any basis of M is infinite.*

Proof. Suppose, by way of contradiction, that $A \subseteq M$ is finite and generates M. Then each element $a \in A$ is a linear combination of some finite subset B_a of B. The union $B' = \bigcup_{a \in A} B_a$ is a finite subset of B that generates M. In particular, any element $b \in B \setminus B'$ is a linear combination of the elements of B' which contradicts the linear independence of B. $\square$

Lemma 2.13. *Let R be any ring, M be a free R-module with infinite bases B_1 and B_2. Then B_1 and B_2 have the same cardinality, that is, there exists a bijection $B_1 \to B_2$.*

Proof. We will use the following facts:

1. If X is an infinite set then X has the same cardinality as the family of all finite subsets of X.
2. If X is an infinite set and Y is a partition of X consisting of finite nonempty subsets then Y has the same cardinality as X.
3. If there exist injections $X \to Y$ and $Y \to X$ then the sets X and Y have the same cardinality.

Thus it suffices to show that there exists an injection from some partition of B_1 consisting of finite nonempty subsets into the family of all finite subsets of B_2.

For each $b \in B_1$, let $\varphi(b)$ be the unique finite subset of B_2 such that $b = \sum_{a \in \varphi(b)} r_a a$ with $r_a \neq 0$ for every $a \in \varphi(b)$. Define an equivalence relation $\sim$ on B_1 so that $b \sim b'$ iff $\varphi(b) = \varphi(b')$. Let P be the set of all equivalence classes of $\sim$ and let ψ be the function assigning to an element $A \in P$ the finite set $\varphi(b)$ with $b \in A$. Then ψ is an injection from P into the family of all finite subsets of B_2. It remains to show that every $A \in P$ is finite.

Arguing as in the proof of Lemma 2.12 we notice that if $A \in P$ then there exists a finite subset of B_1 that spans all the elements of A. Since $A \subseteq B_1$ and B_1 is linearly independent it follows that A is finite. Thus ψ is the required injection and the proof is complete. $\square$

Division Rings.

Theorem 2.14. *Any division ring has the invariant dimension property.*

Proof. Let R be a division ring, M be a free R-module and B_1, B_2 be bases of M. It suffices to assume that B_1 and B_2 are finite. Suppose, by way of contradiction, that B_1 has n elements and B_2 has m elements with $n < m$. Assume that the intersection $B = B_1 \cap B_2$ is as large as possible. Clearly, there exists $b \in B_1 \setminus B$. Let $b = \sum_{a \in B_2} r_a a$ for some $r_a \in R$. There exists

$a_0 \in B_2 \setminus B$ such that $r_{a_0} \neq 0$. Let $B_2' = B_2 \setminus \{a_0\} \cup \{b\}$. Since $b = \sum_{a \in B_2} r_a a$ and $r_{a_0} \neq 0$, we get

$$a_0 = r_{a_0}^{-1} b - \sum_{a \in B_2 \setminus \{a_0\}} r_{a_0}^{-1} r_a a.$$

Thus B_2' spans every element of B_2 hence it spans M. B_2' is linearly independent since b is not spanned by $B_2 \setminus \{a_0\}$. Thus B_2' is a basis of M, it has m elements and the intersection $B_1 \cap B_2' = B \cup \{b\}$ is larger than B. This contradicts the choice of B_1 and B_2 as having the intersection as large as possible. □

Commutative Rings.

Definition. Let R be a ring, M be an R-module and I be an ideal of R. Define IM to be the set of all finite sums $\sum_j i_j m_j$ with $i_j \in I$ and $m_j \in M$ for each j.

Remark. IM is a submodule of M.

Definition. Let R be a ring, M be an R-module and I be an ideal of R. Define scalar multiplication on M/IM be the elements of the ring R/I as follows:

$$(r+I)(m+IM) = rm + IM.$$

Remark. The scalar multiplication is well defined. If $r_1, r_2 \in R$ with $r_1 - r_2 \in I$ and $m_1, m_2 \in M$ with $m_1 - m_2 \in IM$, then

$$r_1 m_1 - r_2 m_2 = (r_1 - r_2) m_1 + r_2 (m_1 - m_2) \in IM.$$

Lemma 2.15. *Let R be a ring, M be a free R-module with basis B and I be a proper ideal of R. Then M/IM is a free (R/I)-module with basis $B' = \{b + IM : b \in B\}$ for any $b_1 \neq b_2$ from B we have $b_1 + IM \neq b_2 + IM$.*

Proof. Clearly B' generates M/IM. Suppose that $b_1, \ldots, b_n \in B$ are distinct and

$$(r_1 + I)(b_1 + IM) + \cdots + (r_n + I)(b_n + IM) = IM.$$

Thus $m = r_1 b_1 + \cdots + r_n b_n \in IM$. Let $i_1, \ldots, i_k \in I$ and $m_1, \ldots, m_k \in M$ be such that $m = i_1 m_1 + \cdots + i_k m_k$. We can express each m_j as a linear combination of the elements of B with coefficients from R. Thus m is a linear combination of the elements of B with coefficients from I. Since B is a basis of M, it follows that $r_1, \ldots, r_n \in I$. Thus B' is linearly independent over R/I. It also follows that $b_1 + IM \neq b_2 + IM$ for any $b_1 \neq b_2$ from B since otherwise

$$(1_R + I)(b_1 + IM) + (-1_R + I)(b_2 + IM) = IM$$

so $1_R \in I$ and $I = R$ contrary to out assumption that I is a proper ideal. □

Theorem 2.16. *Any commutative ring has the invariant dimension property.*

Proof. Let R be a commutative ring. If R is trivial, then any free R-module is trivial so R has the invariant dimension property. Assume that R is nontrivial, M is an R-module and let B_1 and B_2 be any bases of M. Let I be a maximal ideal in R. Then $F = R/I$ is a field and B_1', B_2' are bases of M/IM over F, where $B_i' = \{b + IM : b \in B_i\}$, $i = 1, 2$. Since F has the invariant dimension property, the sets B_1' and B_2' have the same cardinality. It follows that the sets B_1 and B_2 have the same cardinality. □

Semisimple Rings.

Definition. A ring R is semisimple iff it is semisimple as an R-module.

Remark. Note that any free module over a semisimple ring is semisimple. We will show later that semisimple rings also have the invariant dimension property.

The Universal Extension Property for Free Modules.

Lemma 2.17. *If N is a free R-module with a basis B and M is any R-module, then any function $B \to M$ can be uniquely extended to an R-homomorphism $N \to M$.*

Proof. Given $f : B \to M$, let $\varphi : N \to M$ be defined by

$$\varphi\left(r_1 b_1 + \cdots + r_n b_n\right) = r_1 f\left(b_1\right) + \cdots + r_n f\left(b_n\right).$$

□

Remark. Note that if B is any subset of N such that any function from B to an R-module can be extended uniquely to a homomorphism, then N is free with basis B.

Proof. Let $B = \left(b_i : i \in I\right)$, let M be a free module over I and let $D = \left\{d_i : i \in I\right\}$ be a basis of M. Let $f : B \to M$ maps b_i to d_i for each $i \in I$ and let $g : N \to M$ be the unique extension of f to a homomorphism. It suffices to show that g is an isomorphism. □

Arbitrary Modules as Quotients of Free Modules.

Theorem 2.18. *Any R-module is isomorphic to a quotient module of a free R-module.*

Proof. Let M be an R-module, $\left\{m_i : i \in I\right\}$ be any subset of M that generates M and N be a free module over I. If $B = \left\{b_i : i \in I\right\}$ is a basis of N, then let $\varphi : N \to M$ be the unique R-homomorphism that extends the function $f : B \to M$ given by $f\left(b_i\right) = m_i$. Note that φ is surjective. If $N' = \ker\left(\varphi\right)$, then M is isomorphic to N/N'. □

Modules over Semisimple Rings.

Theorem 2.19. *Any module over a semisimple ring is semisimple.*

Proof. Let R be a semisimple ring and M be an R-module. Then M is isomorphic to N/N' for some free R-module N and some submodule N' of N. Then N is semisimple implying that N/N' is semisimple. □

Modules over Division Rings are Free.

Remark. Let R be a division ring. Then R is a simple R-module and it is the unique (up to isomorphism) simple R-module. Any R-module over R is semisimple so it is the direct sum of modules isomorphic to R. Thus any module over a division ring is free.

Maschke's Theorem.

Theorem 2.20. *Let G be a finite group of order n and F be a field whose characteristic does not divide n. Then the group ring $F[G]$ is semisimple.*

Proof. It suffices to show that for every left ideal N of $F[G]$ there exists an $F[G]$-homomorphism $\varphi : F[G] \to F[G]$ such that $\varphi^2 = \varphi$ and $\operatorname{im}(\varphi) = N$. Let N be any left ideal of $F[G]$. Then N is a subspace of $F[G]$ as a vector space over F. Let $b_1, \dots, b_m$ be a basis of N. This basis can be extended to a basis $b_1, \dots, b_m, b_{m+1}, \dots, b_n$ of $F[G]$ (note that the dimension of $F[G]$ over F is n). Let $\pi : F[G] \to F[G]$ be the projection onto N, that is, let

$$\pi\big(a_1 b_1 + \cdots + a_n b_n\big) = a_1 b_1 + \cdots + a_m b_m,$$

where $a_1, \dots, a_n \in F$. Note that π is an F-homomorphism, but not necessarily an $F[G]$-homomorphism. Define $\varphi : F[G] \to F[G]$ as follows:

$$\varphi(t) = \frac{1}{n} \sum_{g \in G} g\pi\left(g^{-1}t\right),$$

for any $t \in F[G]$. Clearly $\varphi^2 = \varphi$ and $\operatorname{im}(\varphi) = N$. It remains to show that φ is an $F[G]$-homomorphism. Let $t \in F[G]$ and $h \in G$. It suffices to show that $\varphi(ht) = h\varphi(t)$. We have

$$\begin{aligned}
\varphi(ht) &= \frac{1}{n} \sum_{g \in G} g\pi\left(g^{-1}ht\right) \\
&= \frac{1}{n} \sum_{g \in G} h\left(h^{-1}g\right)\pi\left(\left(h^{-1}g\right)^{-1} t\right) \\
&= \frac{1}{n} \sum_{g \in G} hg\pi\left(g^{-1}t\right) \\
&= h\varphi(t),
\end{aligned}$$

and the proof is complete. □

3. The Structure of Semisimple Rings.

Simple Left Ideals.

Definition. A simple left ideal of a ring R is a left ideal that is simple as an R-module.

Remark. Equivalently, the simple left ideals of a ring R are the simple submodules of the R-module R.

Lemma 3.1. *Let L be a simple left ideal of a ring R and E be any simple R-module. If E is not isomorphic to L, then $LE = \{0\}$.*

Proof. Note that LE is a submodule of E hence it is either $\{0\}$ or E. Suppose, by way of contradiction, that $LE = E$ and let $a \in E$ be such that $La \neq \{0\}$. Since La is a submodule of E it is equal to E. The map $\varphi : L \to E$ with $\varphi(\alpha) = \alpha a$ is a nonzero homomorphism of R-modules, hence it is an isomorphism which is a contradiction.

Homework 9 (due 10/11).

$\square$

Let V be a vector space over $\mathbb{R}$ of countable dimension, say $V = \mathbb{R}[x]$, and let $R = \operatorname{End}_{\mathbb{R}}(V)$. Prove that the ideal I of R consisting of those $\varphi \in R$ for which the image of φ is a finitely dimensional subspace of V is maximal.

Remark. It follows from the correspondence theorem for rings that R/I has no proper nontrivial ideals. It can be proved that the ring R/I is not semisimple.

Semisimple Rings as Products of Simple Rings.

Definition. A ring R is simple iff it is semisimple and all its simple left ideals are R-isomorphic to each other.

Remark. We will show later that a simple ring has no nontrivial proper ideals and that any semisimple ring that has no nontrivial proper ideals is simple.

Proposition 3.2. *If R is a simple ring, then all simple R-modules are R-isomorphic to each other and to the unique (up to isomorphism) left ideal of R.*

Proof. Let $R = \sum_{i\in I} L_i$ with each L_i being a simple left ideal of R and let M be a simple R-module. Let $m \in M \smallsetminus \{0\}$ and $1_R = \ell_{i_1} + \cdots + \ell_{i_k}$ for some $i_1, \ldots, i_k \in I$. Then

$$m = \ell_{i_1} m + \cdots + \ell_{i_k} m \neq 0$$

so $\ell_{i_j} m \neq 0$ for some $j \in \{1, \ldots, k\}$. Then $L_{i_j} M \neq \{0\}$ so M is R-isomorphic to L_{i_j}. $\square$

Example. Let V be a finitely dimensional vector space over a field F and $R = \operatorname{End}_F(V)$. If $\{b_1, \ldots, b_n\}$ is a basis of V and

$$L = \left\{\varphi \in \operatorname{End}_F(V) : \varphi\left(b_i\right) = 0,\ i = 2, \ldots, n\right\},$$

then L is a simple left ideal of R. It can be proved that any simple left ideal of R is isomorphic to L and that R is semisimple. Thus R is a simple ring.

Theorem 3.3. *Let R be a semisimple ring. Then there are finitely many two-sided ideals $R_1, \ldots, R_k$ of R such that each R_i is a simple ring and R is ring isomorphic to the direct product $\prod_{i=1}^{k} R_i$.*

Remark. The operations of addition and multiplication in the ring R_i are inherited from R, however the multiplicative identity 1_{R_i} does not have to be equal 1_R. Actually, it can't be equal 1_R unless $k = 1$.

Proof. Consider the equivalence relation of R-isomorphism on the set of all simple left ideals of R and let $\{L_i : i \in I\}$ be a set of representatives of the equivalence classes. For each $i \in I$, let R_i be the sum of all simple left ideals of R that are isomorphic to L_i. Clearly, each R_i is a left ideal of R.

Now we show that each R_i is a right ideal. Since R is semisimple, we have $R = \sum_{i \in I} R_i$. If $r_j \in R_j$ for some $j \in I$ and $r \in R$, then $r = r'_j + r'$ with $r'_j \in R_j$ and $r' \in \sum_{i \in I \setminus \{j\}} R_i$ so

$$r_j r = r_j r'_j + r_j r' = r_j r'_j \in R_j.$$

Thus R_j is a right ideal.

Since $R = \sum_{i \in I} R_i$, we have $1_R = e_1 + \cdots + e_k$ with $e_j \in R_{i_j}$ for each $j = 1, \ldots, k$ and some $i_1, \ldots, i_k \in I$. Then $R = \sum_{j=1}^{k} R_{i_j}$. Note that $I = \{i_1, \ldots, i_k\}$, since otherwise if $i \in I \setminus \{i_1, \ldots, i_k\}$, then $R_i R_{i_j} = \{0\}$ for any $j = 1, \ldots, k$ implying that $R_i R = \{0\}$ which is a contradiction. We can thus assume that $i_j = j$ for each $j = 1, \ldots, k$ so $I = \{1, \ldots, k\}$ and $R = \sum_{j=1}^{k} R_j$.

If $r \in R_j$, then

$$r = re_1 + \cdots + re_k = re_j.$$

Similarly $e_j r = r$ so $e_j = 1_{R_j}$ implying that R_j is a a ring for every $j = 1, \ldots, k$. Any left ideal of R_j is a left ideal of R so it is isomorphic to L_j implying that R_j is a simple ring for each $j = 1, \ldots, k$.

If $0 = r_1 + \cdots + r_k$ with $r_j \in R_j$ for every $j = 1, \ldots, k$, then multiplying both sides by some e_j we get $r_j = 0$ implying that $R = \bigoplus_{j=1}^{k} R_j$ as R-modules. It follows that R is isomorphic to $\prod_{j=1}^{k} R_j$ as R-modules with the isomorphism $\varphi : \prod_{j=1}^{k} R_j \to R$ defined by

$$\varphi(r_1, \ldots, r_k) = r_1 + \cdots + r_k.$$

We show that φ is an isomorphism of rings. It remains to show that φ preserves multiplication. We have

$$\begin{aligned}
\varphi(r_1 s_1, \ldots, r_k s_k) &= r_1 s_1 + \cdots + r_k s_k \\
&= (r_1 + \cdots + r_k)(s_1 + \cdots + s_k) \\
&= \varphi(r_1, \ldots, r_k)\varphi(s_1, \ldots, s_k)
\end{aligned}$$

for any $r_j, s_j \in R_j$, $j = 1, \ldots, k$. Thus the proof is complete. $\square$

Corollary 3.4. *If R is a semisimple ring then any simple R-module is R-isomorphic to one of the simple left ideals of R. In particular, there are only finitely many simple R-modules up to R-isomorphism.*

The Structure of Simple Rings.

Lemma 3.5. *Let R be a simple ring. Then R is a finite direct sum of simple left ideals of R. Moreover,*

1. *R has no two-sided ideals except R and $\{0\}$.*
2. *If L_1 and L_2 are simple left ideals of R, then $L_2 = L_1 r$ for some $r \in R$.*

Remark. If follows that $LR = R$ for any nonzero left ideal L of R.

Proof. Since R is semisimple, $R = \bigoplus_{j\in J} L_j$ for some simple left ideals L_j of R. Since 1_R can be expressed as the sum of finitely many $\ell_j \in L_j$, it follows that J is finite. Since 2. $\Rightarrow$ 1., it remains to prove 2.

Let $\varphi : L_1 \to L_2$ be an R-isomorphism, let $R = L_1 \oplus L_1'$ (as R-modules) for some left ideal L_1' of R and let $\pi : R \to L_1$ be the corresponding projection. Consider the composition $\sigma = \varphi \circ \pi : R \to L_2$ and let $r = \sigma\big(1_R\big)$. Note that σ is an R-homomorphism. If $\ell \in L_1$, then

$$\varphi(\ell) = \sigma(\ell) = \sigma\big(\ell \cdot 1_R\big) = \ell \cdot r.$$

Thus $L_2 = L_1 r$. □

Homework 10 (due 10/21).

Prove that 2. $\Rightarrow$ 1. in Lemma 3.5.

The Double Endomorphism Ring.

Remark. Let R be a ring and M be an R-module. Then $R' = \mathrm{End}_R(M)$ is a ring and M has a natural structure of an R'-module with scalar multiplication given by $r'm = r'(m)$ for any $r' \in R'$ and $m \in M$. If $r \in R$, then let $\varphi_r : M \to M$ be given by $\varphi_r(m) = rm$. If $r' \in R'$ and $r \in R$, then

$$r'\left(\varphi_r(m)\right) = r'(rm) = r\left(r'(m)\right) = \varphi_r\big(r'(m)\big)$$

so $\varphi_r \in \mathrm{End}_{R'}(M)$. Moreover, the function $R \to R'' = \mathrm{End}_{R'}(M)$ assigning φ_r to $r \in R$ is a ring homomorphism.

Definition. We call the ring R'' the double endomorphism ring of M over R and the homomorphism $R \to R''$ assigning φ_r to $r \in R$ is called the canonical homomorphism.

Rieffel's Theorem.

Theorem 3.6. *Let R be a ring with no nontrivial proper ideals and let L be a nonzero left ideal of R. If R'' is the double homomorphism ring of L over R, then the canonical ring homomorphism $\lambda : R \to R''$ is an isomorphism.*

Proof. λ is nonzero so its kernel is a proper ideal of R. Thus $\ker(\lambda)$ is trivial implying that λ is injective. It remains to show that λ is surjective.

First we show that $\lambda(L)$ is a left ideal of R''. Given $r \in R$ let $\psi_r : L \to L$ be the right multiplication by r, that is let $\psi_r(\ell) = \ell r$ for any $\ell \in L$. Then

$$\psi_r(s\ell) = (s\ell)\, r = s\,(\ell r) = s\psi_r(\ell)$$

for any $s \in R$ and $\ell \in L$ implying that $\psi_r \in R' = \mathrm{End}_R(L)$. If $\ell, \ell' \in L$ and $f \in R'' = \mathrm{End}_{R'}(L)$, then

$$\big(f \circ \lambda(\ell)\big)\big(\ell'\big) = f\big(\ell\ell'\big) = f\big(\psi_{\ell'}(\ell)\big) = \psi_{\ell'}\big(f(\ell)\big) = f(\ell)\ell' = \varphi_{f(\ell)}\big(\ell'\big)$$

so $f \circ \lambda(\ell) = \varphi_{f(\ell)} \in \lambda(L)$ implying that $\lambda(L)$ is a left ideal of R''.

Since LR is a nonzero two-sided ideal of R it follows that $LR = R$ which implies that $\lambda(L)\lambda(R) = \lambda(R)$. Since $\lambda(L)$ is a left ideal of R'' we have $R''\lambda(L) = \lambda(L)$. Consequently

$$R'' = R''\lambda(R) = R''\lambda(L)\lambda(R) = \lambda(L)\lambda(R) = \lambda(R)$$

completing the proof. □

4. Complex Representations of Finite Groups.

The Simple Factors of the Group Ring.

Let F be an algebraically closed field of characteristic 0, let G be a finite group and n be the order of G. Then the group ring $F[G]$ is semisimple so

$$F[G] \cong R_1 \times \ldots \times R_s$$

for some simple rings $R_1, \ldots, R_s$. Let L_i be a simple left ideal of R_i for each $i = 1, \ldots, s$. Each R_i and each L_i is a vector space over F. Let d_i be the dimension of L_i over F for each $i = 1, \ldots, s$.

Lemma 4.1. *We have $R_i \cong End_F\big(L_i\big)$ for each $i = 1, \ldots, s$.*

Proof. Fix $i \in \{1, \ldots, s\}$ and let $R_i' = \mathrm{End}_{R_i}\big(L_i\big)$. Since L_i is a simple R_i-module, the ring R_i' is a division ring. Identifying each element $a \in F$ with the scalar multiplication by a we have $F \subseteq R_i'$. We claim that $F = R_i'$.

Suppose, by way of contradiction, that $a \in R_i' \setminus F$. Since a commutes with any element of F, the subring $F[a]$ of R_i' generated by $a \cup F$ is commutative. $F[a]$ is a subring of a division ring so it has no zero divisors. Thus $F[a]$ is an integral domain. Any inverse of a nonzero element of $F[a]$ is in R_i' so R_i' contains a subring $F(a)$ that is the field of fractions of $F[a]$. (Actually $F(a) = F[a]$.) $F(a)$ has finite dimension over F so a is algebraic over F. Since F is algebraically closed, it follows that $a \in F$ which is a contradiction. Thus the claim is proved.

Since the ring R_i is simple, it has no nontrivial proper two-sided ideals. Moreover, L_i is a nonzero left ideal of R_i. If $R_i'' = \mathrm{End}_{R_i'}\big(L_i\big)$ is the double homomorphism ring of L_i over R_i, then Rieffel's Theorem implies that the canonical ring homomorphism $\lambda : R_i \to R_i''$ is an isomorphism. Since $R_i' \cong F$ the proof is complete. □

Corollary 4.2. *We have*

$$n = d_1^2 + \cdots + d_s^2.$$

Proof. The dimension of $F[G]$ over F is n and the dimension of R_i over F is d_i^2 for each $i = 1, \ldots, s$. □

Theorem 4.3. *The index s is equal to the number of conjugacy classes of G.*

Proof. Let A be the center of $F[G]$, that is, let A be the set of all the elements $a \in F[G]$ such that $ab = ba$ for every $b \in F[G]$. Then A is a subspace of $F[G]$ as a vector space over F. An element $\sum_{g \in G} a_g g \in F[G]$ belongs to A if and only if $a_g = a_h$ whenever g and h are conjugates in G. Thus the dimension of A over F is equal to the number of conjugacy classes of G.

For each $i = 1, \ldots, s$ let A_i be the center of R_i. Then $A \cong A_1 \times \ldots \times A_s$ and each A_i has dimension 1 over F. Thus the dimension of A over F is equal to s completing the proof. □

Homework 12 (due 11/4).

Prove that each A_i has dimension 1 over F.

Examples.

1. Let $G = S_3$. Then $s = 3$, $d_1 = d_2 = 1$ and $d_3 = 2$ are the only solutions of $d_1^2 + d_2^2 + d_3^2 = 6$ (up to a permutation of d_1, d_2, d_3. A possible isomorphism $\varphi : F[G] \to R_1 \times R_2 \times R_3$ is given by

$$\begin{aligned} \varphi(1\,2\,3) &= \left([1], [1], \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}\right) \\ \varphi(2\,3) &= \left([1], [-1], \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\right) \end{aligned}$$

2. Let G be a cyclic group of order n. Then $s = n$ and $d_1 = \cdots = d_n = 1$. A possible isomorphism $\varphi : F[G] \to R_1 \times \ldots \times R_n$ is given by

$$\varphi(g) = \left([1], [\zeta], [\zeta^2], \ldots, [\zeta^{n-1}]\right)$$

where g is a generator of G and ζ is a primitive root of 1 in F of degree n.

Proof of Lemma 2.2 (the Key Result for Burnside's Theorem).

Algebraic Integers.

Definition. An algebraic integer is a root of a nonzero monic polynomial with integer coefficients.

Theorem 4.4. *The set $\mathbb{I}$ of algebraic integers is a subring of $\mathbb{C}$ such that $\mathbb{I} \cap \mathbb{Q} = \mathbb{Z}$.*

Remark. The proof of Theorem 4.4 will be given later.

Irreducible Complex Representations and their Characters.

Definition. Let G be a finite group of order n with s conjugacy classes and let

$$\varphi : \mathbb{C}[G] \to R_1 \times \ldots \times R_s$$

be a ring isomorphism, where R_i is the ring of $d_i \times d_i$ complex matrices for each $i = 1, \ldots, s$. Let $\rho_i : \mathbb{C}[G] \to R_i$ be the composition $\pi_i \circ \varphi$, where π_i is the projection on the i-th coordinate, $i = 1, \ldots, s$. Let $\chi_i : \mathbb{C}[G] \to \mathbb{C}$ be the composition $\mathrm{tr}_i \circ \rho_i$ where $\mathrm{tr}_i : R_i \to \mathbb{C}$ assigns to each matrix in R_i its trace (sum of all elements on the main diagonal). Then $\rho_1, \ldots, \rho_s$ are the irreducible complex representations of G and $\chi_1, \ldots, \chi_s$ are theirs characters.

Theorem 4.5. *For every $g \in G$ and every $i = 1, \ldots, s$, the character $\chi_i(g)$ is the sum of d_i roots of unity of degree n. If $\chi_i(g) = d_i \zeta$ for some root of unity ζ, then $\rho_i(g)$ is equal to ζ multiplied by the $d_i \times d_i$ identity matrix. In particular, $\chi_i(g)$ is an algebraic integer.*

Remark. The proof of Theorem 4.5 will be given later.

Theorem 4.6. *If $g, h \in G$ are in different conjugacy classes, then*

$$\sum_{i=1}^{s} \chi_i(g) \chi_i(h^{-1}) = 0.$$

Remark. The proof of Theorem 4.6 will be given later.

Theorem 4.7. *If C is a conjugacy class of G and $g \in C$ then $|C| \chi_i(g)/d_i$ is an algebraic integer for every $i = 1, \ldots, s$.*

Remark. The proof of Theorem 4.7 will be given later.

Lemma 4.8. *If C is a conjugacy class of G such that $|C|$ is relatively prime to d_i for some $i \in \{1, \ldots, s\}$ and $g \in C$, then either $\chi_i(g) = 0$ or $\rho_i(g)$ is a constant multiple of the identity matrix.*

Proof. There exist integers m and ℓ such that $md_i + \ell |C| = 1$. Thus

$$\frac{\chi_i(g)}{d_i} = m\chi_i(g) + \ell |C| \frac{\chi_i(g)}{d_i}$$

is an algebraic integer. Let $\zeta \in \mathbb{C}$ be a primitive root of unity of degree n and let H be the Galois group of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. Since $\chi_i(g)$ is a sum of d_i roots of unity from the field $\mathbb{Q}(\zeta)$, it follow that if $h \in H$ then $h(\chi_i(g))$ is also a sum of d_i roots of unity from $\mathbb{Q}(\zeta)$. Let $N : \mathbb{Q}(\zeta) \to \mathbb{Q}$ be the norm on $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. Let

$$\beta = N\left(\frac{\chi_i(g)}{d_i}\right) = \prod_{h \in H} h\left(\frac{\chi_i(g)}{d_i}\right) = \prod_{h \in H} \frac{h(\chi_i(g))}{d_i}.$$

Applying the absolute value and using the inequality

$$\left|\frac{h\big(\chi_i(g)\big)}{d_i}\right| \leq 1$$

we get $\left|\beta\right| \leq 1$. Since the ring of algebraic integers is closed under conjugation, it follows that $\left|\beta\right|^2$ is an integer. Thus $\left|\beta\right| = 0$ or $\left|\beta\right| = 1$.

If $\left|\beta\right| = 0$, then $\chi_i\big(g\big) = 0$. Assume that $\left|\beta\right| = 1$. Since $\chi_i\big(g\big)$ is the sum of d_i roots of unity and since roots of unity have absolute value 1, there is a root of unity ξ such that $\chi_i\big(g\big) = d_i\xi$. Thus $\rho_i\big(g\big)$ is the $d_i \times d_i$ matrix with ξ along the main diagonal and zeros outside it. □

The completion of the Proof of Lemma 2.2

Proof. Assume that G is a finite non-abelian simple group. Suppose, by way of contradiction that C is a conjugacy class of G of order p^a with p being a prime integer and a being a positive integer. Assume that ρ_1 is the unit representation (with $\rho_1\big(g\big)$ being the 1×1 identity matrix for all $g \in G$). In particular $d_1 = 1$.

We claim that if $i \in \{2, \ldots, s\}$ is such that p does not divide d_i, then $\chi_i\big(g\big) = 0$ for every $g \in C$. Suppose that the claim holds. Let $J = \big\{i \in \{2, \ldots, s\} : p|d_i\big\}$ and let $d_i = pb_i$ for each $i \in J$. Since

$$\sum_{i=1}^{s} \chi_i\big(g\big)\chi_i\big(1_G\big) = 0$$

for $g \in C$, and since $\chi_i\big(1_G\big) = d_i$, it follows that

$$1 + p\sum_{i \in J} b_i\chi_i\big(g\big) = 0.$$

Since each $\sum_{i \in J} b_i\chi_i\big(g\big)$ is an algebraic integer, it follows that $1/p$ is an algebraic integer which is a contradiction.

It remains to prove the claim. Suppose that the claim fails. Then there is some $i \in \{2, \ldots, s\}$ and $g \in C$ such that p does not divide d_i and $\chi_i\big(g\big) \neq 0$. Then $\rho_i\big(g\big)$ is a constant multiple of the identity matrix. Let

$$H = \big\{g \in G : \rho_i\big(g\big) \text{ is a constant multiple of the identity matrix}\big\}.$$

Then H is a nontrivial normal subgroup of G implying that $H = G$. Consider the image $\rho_i(G) \subseteq R_i$. It is an abelian group under the multiplication of R_i and ρ_i restricted to G is a group homomorphism $G \to \rho_i(G)$. Since ρ_i is not the trivial representation, it follows that $\ker\big(\rho_i\restriction G\big) \neq G$. Thus the kernel of $\rho_i\restriction G$ is trivial implying that $\rho_i\restriction G$ is injective and consequently that $\rho_i(G)$ is isomorphic to G. Since $\rho_i(G)$ is abelian and G is not abelian, we have a contradiction. Thus the claim is proved. □

Integral Extensions of Commutative Rings.

Cofactors of a Matrix.

Definition. Let R be a commutative ring and A be a square $n \times n$ matrix over R. For each $i, j \in \{1, \ldots, n\}$ let b_{ji} be equal to $(-1)^{i+j} \det\left(A_{ij}\right)$, where A_{ij} is the $(n-1) \times (n-1)$ matrix obtained from A by removing the i-th row and the j-th column. The resulting $n \times n$ matrix B with entries b_{ji} is called the matrix of cofactors of A.

Remark. We have $AB = BA = \det(A) \cdot I_n$, where I_n is the $n \times n$ identity matrix.

Integral Elements.

Definition. Let S be a nontrivial commutative ring, R be a subring of S and $a \in S$. We say that a is integral over R if there exists a monic polynomial $f \in R[x]$ with root a.

Theorem 4.9. *Let S be a nontrivial commutative ring, R be a subring of S and $a \in S$. Then the following conditions are equivalent:*

1. *a is integral over R;*
2. *the subring $R[a]$ of S is finitely generated as an R-module.*
3. *there exists a subring T of S that is finitely generated as an R-module and contains $R[a]$.*

Proof. 1. $\Rightarrow$ 2. Assume that a is a root of

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x].$$

Then $1_R, a, a^2, \ldots, a^{n-1}$ generate $R[a]$ as an R-module so $R[a]$ is finitely generated.

2. $\Rightarrow$ 3. Take $T = R[a]$.

3. $\Rightarrow$ 1. Assume that that $b_1, \ldots, b_k$ generate T as an R-module. Consider the function $\varphi : T \to T$ given by $\varphi(m) = am$. Then φ is an R-homomorphism. Let $t_{ij} \in R$ be such that

$$\varphi\left(b_i\right) = ab_i = t_{i1}b_1 + \cdots + t_{ik}b_k$$

for each $i = 1, \ldots, k$. Consider the matrix

$$A = \begin{bmatrix} a - t_{11} & -t_{12} & -t_{13} & \cdots & -t_{1k} \\ -t_{21} & a - t_{22} & -t_{23} & \cdots & -t_{2k} \\ -t_{31} & -t_{32} & a - t_{33} & \cdots & -t_{3k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -t_{k1} & -t_{k2} & -t_{k3} & \cdots & a - t_{kk} \end{bmatrix}$$

and let B be the matrix of cofactors of A. Then the product BA is equal to the identity matrix multiplied by $\det(A)$. Any linear combination of $b_1, \ldots, b_k$ with coefficients taken from a row of BA is equal to 0. Thus $\det(A) \cdot b_i = 0$ for each $i = 1, \ldots, k$. Since 1_s is a linear combination of $b_1, \ldots, b_k$ with coefficients from R, it follows that $\det(A) = 0$. Let

$f(x) \in R[x]$ be the polynomial obtained by calculating the determinant of the following matrix over $R[x]$

$$\begin{bmatrix} x-t_{11} & -t_{12} & -t_{13} & \cdots & -t_{1k} \\ -t_{21} & x-t_{22} & -t_{23} & \cdots & -t_{2k} \\ -t_{31} & -t_{32} & x-t_{33} & \cdots & -t_{3k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -t_{k1} & -t_{k2} & -t_{k3} & \cdots & x-t_{kk} \end{bmatrix}.$$

Then f is monic and a is a root of f. □

Integral Elements Form a Subring.

Theorem 4.10. *Let S be a nontrivial commutative ring and R be a subring of S. Let T be the subset of S consisting of all elements $a \in S$ that are integral over R. Then T is a subring of S containing R.*

Proof. Clearly T contains R. Assume that $a, b \in T$. Then $R[a]$ is generated by some $a_1, \ldots, a_k \in S$ as an R-module and $R[b]$ is generated by some $b_1, \ldots, b_\ell$ as R-module. Then the products $a_i b_j$ generate $R[a, b]$ implying that $R[a, b] \subseteq T$. Thus $a + b$, $a - b$, and ab belong to T. □

Corollary 4.11. *The algebraic integers form a subring of $\mathbb{C}$.*

Proof. Use Theorem 4.10 with $S = \mathbb{C}$ and $R = \mathbb{Z}$. Then T is the set of all algebraic integers so it is a subring of $\mathbb{C}$ containing $\mathbb{Z}$. □

Integral Elements over a Unique Factorization Domains.

Theorem 4.12. *Let R be a unique factorization domain, F be the field of fractions of R and a be an element of some field extension of F. Then a is integral over R if and only if it is algebraic over F and its minimal polynomial over F has coefficients in R.*

Proof. If a is algebraic over F and its minimal polynomial over F has coefficients in R, then it is clear that a is integral over R.

Assume that a is integral over R. Let $f(x) \in R[x]$ be a monic polynomial with $f(a) = 0$. Let $g(x) \in F[x]$ be the minimal polynomial of a over F. There exists $h(x) \in F[x]$ such that $f(x) = g(x)h(x)$. Let $b \in R$ be such that $bg(x)$ is a primitive polynomial in $R[x]$. Let $c \in F$ be such that $b^{-1}ch(x)$ is a primitive polynomial in $R[x]$. By Gauss lemma, it follows that

$$cf(x) = \big(bg(x)\big)\big(b^{-1}ch(x)\big)$$

is primitive in $R[x]$. Since $f(x)$ is primitive in $R[x]$ it follows that c is a unit in R. Without loss of generality, we can assume that $c = 1$. Thus

$$f(x) = \big(bg(x)\big)\big(b^{-1}h(x)\big)$$

which implies that b is a unit in R. It follows that $g(x) \in R[x]$ and the proof is complete. □

Corollary 4.13. *An algebraic integer belongs to $\mathbb{Q}$ if and only if it belongs to $\mathbb{Z}$.*

Proof. Clearly any integer is an algebraic integer. If a is an algebraic integer in $\mathbb{Q}$, then its minimal polynomial over $\mathbb{Q}$ is $x - a$. Hence $a \in \mathbb{Z}$. $\square$

Remark. Theorem 4.4 now follows.

Finitely Dimensional Complex Representations and their Characters.

Trace of Linear Functions.

Lemma 4.14. *Let V be a finitely dimensional vector space over a field F and $\varphi \in End_F(V)$. Let $b_1, \ldots, b_n$ be a basis of V and, for each $i, j = 1, \ldots, n$, let $a_{ij} \in F$ be such that*

$$\varphi\big(b_i\big) = \sum_{j=1}^{n} a_{ij} b_j.$$

Let $b_1', \ldots, b_n'$ be also a basis of V and, for each $i, j = 1, \ldots, n$, let $a_{ij}' \in F$ be such that

$$\varphi\big(b_i'\big) = \sum_{j=1}^{n} a_{ij}' b_j'.$$

Then

$$a_{11} + a_{22} + \cdots + a_{nn} = a_{11}' + a_{22}' + \cdots + a_{nn}'.$$

Definition. Let V be a finitely dimensional vector space over a field F and $\varphi \in \mathrm{End}_F(V)$. Let $b_1, \ldots, b_n$ be a basis of V and let

$$\varphi\big(b_i\big) = \sum_{j=1}^{n} a_{ij} b_j$$

for each $i = 1, \ldots, n$. The trace of φ, denoted $\mathrm{tr}\big(\varphi\big)$ is equal to the sum $a_{11} + a_{22} + \cdots + a_{nn}$.

Remark. The value of the trace of φ does not depend on the choice of basis for V.

Characters of Finitely Dimensional Complex Representations.

Definition. Let G be a finite group of order n and V be a finitely dimensional complex vector space. Let $\rho : \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V)$ be ring homomorphism, that is, let ρ be a finitely dimensional complex representation of G. The character of ρ, denoted χ_ρ is a map $\chi_\rho : \mathbb{C}[G] \to \mathbb{C}$ such that $\chi_\rho(a)$ is the trace of $\rho(a)$ for each $a \in \mathbb{C}[G]$. The representation ρ is irreducible iff the corresponding $\mathbb{C}[G]$-module on V is simple.

Remarks

1. If ρ is irreducible, then there exists a simple left ideal L of $\mathbb{C}[G]$ and a $\mathbb{C}[G]$-isomorphism $V \to L$.

2. If s is the number of conjugacy classes of G and $L_1, \ldots, L_s$ are all the simple left ideals of $\mathbb{C}[G]$ up to $\mathbb{C}[G]$-isomorphism, then the corresponding representations $\rho_i : \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(L_i)$ (where $a \in \mathbb{C}[G]$ is mapped to the left multiplication by a) are all the irreducible representations of G over $\mathbb{C}$.

3. Let $\mathbb{C}[G] \to R_1 \times \ldots \times R_s$ be a ring isomorphism where $R_1, \ldots, R_s$ are simple rings with the simple left ideals of R_i isomorphic to L_i for each i. Each R_i is isomorphic to a ring of $d_i \times d_i$ matrices over $\mathbb{C}$. If $\rho : \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V)$ is any representation of G, then as a $\mathbb{C}[G]$-module V is a direct sum of simple $\mathbb{C}[G]$-modules. Thus there exists a basis of V over $\mathbb{C}$ so that the values of ρ are matrices of the form

$$\begin{bmatrix} A_1 & 0 & 0 & \cdots & 0 \\ 0 & A_2 & 0 & \cdots & 0 \\ 0 & 0 & A_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \\ 0 & 0 & 0 & \cdots & A_t \end{bmatrix}$$

where each A_i is a $d_j \times d_j$ matrix for some $j \in \{1, \ldots, s\}$.

4. If G is abelian, then each d_i is equal to 1 so there exists a basis of V over $\mathbb{C}$ such that the values of ρ correspond to diagonal matrices. If $g \in G$, then the matrix corresponding to $\rho(g)$ has roots of unity of degree n on the main diagonal.

5. If G is any finite group of order n and $g \in G$, then let H be the cyclic subgroup of G generated by g. Consider the restriction ρ' of ρ to $\mathbb{C}[H]$. There exists a basis of V over F so that all the values of ρ' correspond to diagonal matrices. Then the matrix corresponding to $\rho(g) = \rho'(g)$ has roots of unity of degree n on the main diagonal.

6. If $g \in G$, then $\chi_i(g)$ is the sum of d_i roots of unity of degree n. If $\chi_i(g) = d_i\zeta$ for some root of unity ζ, then there exists a basis of V with respect to which the matrix corresponding to $\rho_i(g)$ is is equal to ζ multiplied by the $d_i \times d_i$ identity matrix. Such a matrix commutes with any $d_i \times d_i$ matrix implying that the form of this matrix does not depend on the choice of basis for V.

7. The proof of Theorem 4.5 is now complete.

The Regular Representation.

Let G be a finite group of order n. The regular representation of G is the representation corresponding to the $\mathbb{C}[G]$-module $\mathbb{C}[G]$. Its character is called the regular character.

Lemma 4.15. *Let $\chi_1, \dots, \chi_s$ be the characters of the irreducible representations of G and χ_r be the character of the regular representation of G. Then*

$$\chi_r = \sum_{i=1}^{s} d_i \chi_i.$$

Lemma 4.16. *Let χ_r be the character of the regular representation of G. Then $\chi_r(g) = 0$ if $g \in G \smallsetminus \{1_G\}$ and $\chi_r(1_G) = n$.*

Proof. Let $G = \{g_1, \dots, g_n\}$ with $g_1 = 1_G$ and let $\rho_r : \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}[G])$ be the regular representation. Note that ρ_r maps an element c of $\mathbb{C}[G]$ to the function $\mathbb{C}[G] \to \mathbb{C}[G]$ that is the multiplication by c (this function is linear, considering $\mathbb{C}[G]$ as a vector space over $\mathbb{C}$). Consider the elements of G as a basis of $\mathbb{C}[G]$ over $\mathbb{C}$. Then $\chi_r(g_i)$ is the trace of the matrix of $\rho_r(g_i)$ with respect to that basis. If $i \neq 1$, then the multiplication by g_i has no fixed points in G implying that every entry on the main diagonal of the matrix corresponding to $\rho_r(g_i)$ is 0 and consequently that $\chi_r(g_i) = 0$. If $i = 1$, then every entry on the diagonal is 1 implying that $\chi_r(g_1) = n$. □

Proof of Theorem 4.6.

We want to show that if $g, h \in G$ are in different conjugacy classes, then

$$\sum_{i=1}^{s} \chi_i(g)\chi_i(h^{-1}) = 0.$$

If e_i is the multiplicative identity of R_i, then

$$\chi_r(e_i h^{-1}) = \sum_{j=1}^{s} d_j \chi_j(e_i h^{-1}) = d_i \chi_i(e_i h^{-1}) = d_i \chi_i(h^{-1}) = \sum_{j=1}^{s} \chi_j(e_i)\chi_j(h^{-1}).$$

Let $g_1, g_2, \dots, g_\ell$ be all the conjugates of g. Then

$$c = \sum_{k=1}^{\ell} g_k = \sum_{i=1}^{s} a_i e_i$$

for some $a_i \in \mathbb{C}$, $i = 1, \dots, s$. Now we get

$$\chi_r(ch^{-1}) = \sum_{k=1}^{\ell} \chi_r(g_k h^{-1}) = 0$$

and

$$\begin{aligned}
\chi_r\left(ch^{-1}\right) &= \sum_{i=1}^{s} a_i \chi_r\left(e_i h^{-1}\right) \\
&= \sum_{i=1}^{s} a_i \sum_{j=1}^{s} \chi_j\left(e_i\right)\chi_j\left(h^{-1}\right) \\
&= \sum_{j=1}^{s} \chi_j\left(\sum_{i=1}^{s} a_i e_i\right)\chi_j\left(h^{-1}\right) \\
&= \sum_{j=1}^{s} \chi_j\left(\sum_{k=1}^{\ell} g_k\right)\chi_j\left(h^{-1}\right) \\
&= \ell \sum_{j=1}^{s} \chi_j(g)\chi_j\left(h^{-1}\right).
\end{aligned}$$

It follows that $\sum_{j=1}^{s} \chi_j(g)\chi_j\left(h^{-1}\right) = 0$.

Proof of Theorem 4.7.

If C is a conjugacy class of G and $g \in C$. We want to show that $|C|\,\chi_i(g)/d_i$ is an algebraic integer for every $i = 1,\dots,s$.

Let $\{g_1,\dots,g_\ell\}$ be the conjugacy class of G containing g. Note that

$$|C|\,\chi_i(g) = \ell\chi_i(g) = \chi_i(g_1) + \cdots + \chi_i(g_\ell) = \chi_i(g_1 + \cdots + g_\ell).$$

Let $C_1,\dots,C_s$ be all the conjugacy classes of G, let $\ell_j = \left|C_j\right|$ for every $j = 1,\dots,s$ and let

$$c_j = g_{j1} + g_{j2} + \cdots + g_{j\ell_j}$$

for every $j = 1,\dots,s$, where $g_{j1},\dots,g_{j\ell_j}$ are the elements of the conjugacy class C_j. Since

$$|C|\,\chi_i(g)/d_i = \chi_i(c_j)/d_i$$

for some $j \in \{1,\dots,s\}$, it suffices to show that:

(∗) the submodule of $\mathbb{C}$ (over $\mathbb{Z}$) generated by the finite set

$$\left\{\chi_i(c_j)/d_i : j = 1,\dots,s\right\}$$

is a subring of $\mathbb{C}$.

Note that for each $j \in \{1,\dots,s\}$ the element c_j belongs to the center of the ring $\mathbb{C}[G]$ implying that the matrix corresponding to $\rho_i(c_j)$ is a constant multiple of the identity matrix. This constant is equal to $\chi_i(c_j)/d_i$. The product $c_j \cdot c_{j'}$ for some $j, j' \in \{1,\dots,s\}$ is also in the center of $\mathbb{C}[G]$ so it is a linear combination of $c_1, \ldots, c_s$ with integer coefficients. It follows that $\rho_i(c_j) \cdot \rho_i(c_{j'})$ is a linear combination of $\rho_i(c_1), \ldots, \rho_i(c_s)$ with the same integer coefficients and consequently that the product

$$\left(\chi_i(c_j)/d_i\right) \cdot \left(\chi_i(c_{j'})/d_i\right)$$

is a linear combination of $\chi_i(c_1)/d_i, \ldots, \chi_i(c_s)/d_i$ with coefficients from $\mathbb{Z}$. The claim $(*)$ follows.

A Divisibility Relation.

Let G be a finite group of order n and $Z_{\mathbb{C}}(G)$. We have $\mathbb{C}[G] \cong R_1 \times \ldots \times R_s$ where R_i is the ring of $d_i \times d_i$ complex matrices. Each R_i corresponds (under this isomorphism) to an ideal (we denote is by R_i as well) of $\mathbb{C}[G]$ which is also a ring. Let e_i be the multiplicative identity of R_i.

Lemma 4.17. *For each $i = 1, \ldots, s$, if*

$$e_i = \sum_{g \in G} a_g g \in \mathbb{C}[G]$$

with $a_g \in \mathbb{C}$ then

$$a_g = \frac{1}{n}\chi_r(e_i g^{-1}) = \frac{d_i}{n}\chi_i(g^{-1}),$$

where χ_r is the regular representation of G.

Proof. Let $g \in G$ and $i \in \{1, \ldots, s\}$ be fixed. Then

$$\chi_r(e_i g^{-1}) = \chi_r\left(\sum_{h \in G} a_h h g^{-1}\right) = \sum_{h \in G} a_h \chi_r(h g^{-1}).$$

Since $\chi_r(hg^{-1}) = 0$ for $h \neq g$ and $\chi_r(hg^{-1}) = n$ when $h = g$, we get

$$\chi_r(e_i g^{-1}) = n a_g,$$

so

$$a_g = \frac{1}{n}\chi_r(e_i g^{-1}).$$

Since

$$\chi_r(e_i g^{-1}) = \sum_{j=1}^{s} d_j \chi_j(e_i g^{-1})$$

and since $\chi_j(a) = 0$ for any $a \in R_k$ with $k \neq j$, we get

$$\chi_r(e_i g^{-1}) = d_i \chi_i(e_i g^{-1}) = d_i \chi_i(g^{-1})$$

and consequently

$$d_i \chi_i(g^{-1}) = n a_g.$$

Thus

$$a_g = \frac{d_i}{n}\chi_i(g^{-1}).$$

□

Faithful Modules.

Definition. Let R be a ring. An R-module M is faithful iff for every $a \in R \setminus \{0\}$ there exists $m \in M$ such that $am \neq 0$.

Remark. Any nontrivial ring is a faithful module over itself.

Theorem 4.18. *Let S be a nontrivial commutative ring, R be a subring of S and $a \in S$. Then a is integral over R iff there exists a faithful $R[a]$-module that is finitely generated as an R-module.*

Proof. Assume that a is integral over R. Then $R[a]$ is a faithful $R[a]$-module that is finitely generated as an R-module.

Assume that M is a faithful $R[a]$-module that is finitely generated as an R-module. Assume that that $b_1, \dots, b_k$ generate M as an R-module. Consider the function $\varphi : M \to M$ given by $\varphi(m) = am$. Then φ is an R-homomorphism. Let $t_{ij} \in R$ be such that

$$\varphi\big(b_i\big) = ab_i = t_{i1}b_1 + \cdots + t_{ik}b_k$$

for each $i = 1, \dots, k$. Consider the matrix

$$A = \begin{bmatrix} a - t_{11} & -t_{12} & -t_{13} & \cdots & -t_{1k} \\ -t_{21} & a - t_{22} & -t_{23} & \cdots & -t_{2k} \\ -t_{31} & -t_{32} & a - t_{33} & \cdots & -t_{3k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -t_{k1} & -t_{k2} & -t_{k3} & \cdots & a - t_{kk} \end{bmatrix}$$

Arguing as in the proof that 3. $\Rightarrow$ 1. in Theorem 4.9, we conclude that $\det(A) \cdot b_i = 0$ for each $i = 1, \dots, k$. Thus $\det(A) \cdot m = 0$ for every $m \in M$. Since M is a faithful $R[a]$-module it follows that $\det(A) = 0$. As in the proof that 3. $\Rightarrow$ 1. in Theorem 4.9 if follows that a is integral over R. □

Corollary 4.19. *For each $i = 1, \dots, s$ the integer d_i divides n.*

Proof. Let ζ be a primitive root of unity of degree n. Consider $\mathbb{C}[G]$ as a $\mathbb{Z}$-module and let M be the submodule generated by the finite set

$$\big\{\zeta^k g e_i : k \in \{0, \dots, n-1\},\, g \in G,\, i \in \{1, \dots, s\}\big\}.$$

Since

$$\frac{n}{d_i} e_i = \sum_{g \in G} \chi_i\big(g^{-1}\big) g e_i$$

and since

$$\chi_i\big(g^{-1}\big) = \zeta^{k_1} + \zeta^{k_2} + \cdots + \zeta^{k_{d_i}}$$

for some $k_1, \dots, k_{d_i} \in \{0, \dots, n-1\}$, it follows that the operation of multiplication by n/d_i maps elements of M to elements of M. Thus M is a $\mathbb{Z}\big[n/d_i\big]$-module. Since $\mathbb{Z}\big[n/d_i\big] \subseteq \mathbb{C}$ it is clear that M is faithful as a $\mathbb{Z}\big[n/d_i\big]$-module. It follows that n/d_i is an algebraic integer. □

Homework 13 (due 12/4).

What is the value of

$$\sum_{i=1}^{s} \chi_i(g)\chi_i(h^{-1})$$

when $g, h \in G$ are in the same conjugacy class? Prove the formula you give.

Homework 14 (due 12/6).

Let G be a finite group of order n with s conjugacy classes and let $\chi_1 \ldots, \chi_s$ be the characters of the irreducible representations of G over $\mathbb{C}$. Prove that the sum

$$\sum_{g \in G} \chi_i(g)\chi_j(g^{-1})$$

is equal to zero when $i \neq j$ and it is equal to n when $i = j$.