A Course In Group Rings

Dr. Leo Creedon

Semester II, 2003-2004

Contents

Chapter 1

Introduction

1.1 Definitions and examples of Rings and Group Rings

Definition 1.1 *A **ring** is a set R with two binary operations $+$ and $\cdot$ such that*

(i) $a + (b + c) = (a + b) + c$

(ii) $\exists\, 0 \in R$ *s.t.* $a + 0 = a = 0 + a$

(iii) $\exists - a \in R$ *s.t.* $a + (-a) = 0 = (-a) + a$

(iv) $a + b = b + a$

(v) $a.(b.c) = (a.b).c$

(vi) $a.(b + c) = a.b + b.c$

(vii) $(a + b).c = a.c + b.c \quad \forall\, a, b, c \in R$

Definition 1.2 *If $a.b = b.a \;\forall\, a, b \in R$, then R is a **commutative ring**.*

Example 1.3 *$(\mathbb{Z}, +, \cdot)$ is a commutative ring.*

Example 1.4 *The set P of polynomials of any degree over $\mathbb{R}$ is a ring (with the obvious multiplication and addition). This is also a commutative ring e.g. $(2x^2 + 1)(3x + 2) = (3x + 2)(2x^2 + 1) \in P$.*

Definition 1.5 *If* $\exists 1 \in R$ *such that* $1.a = a.1 \ \forall \ a \in R$, *then* R *is a* ***ring with identity****. Otherwise* R *is a ring without identity.*

For us, R (usually) is a ring with identity.

Example 1.6 *The set* $M_n(\mathbb{R})$ *of all* $n \times n$ *matrices with real coefficients is a ring (with matrix addition and matrix multiplication).*

(i) $A + (B + C) = (A + B) + C \quad \checkmark$

(ii) *Let* $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, *then* $0 + A = A + 0 = A \quad \checkmark$

(iii) *If* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,*then* $-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ *and* $-A + A = A + -A = 0 \quad \checkmark$

(iv) $A + B = B + A \quad \checkmark$

(v) $A.(\,B.C\,) = (\,A.B\,).C \quad \checkmark$

(vi) $A.(\,B + C\,) = A.B + B.C \quad \checkmark$

(vii) $(\,A + B\,).C = A.C + B.C \quad \forall \ A, B, C \in M_n(\mathbb{R}) \quad \checkmark$

Note : $M_n(\mathbb{R})$ is a non-commutative ring (since $AB \neq BA \ \forall \ A, B \in M_n(\mathbb{R})$).

Example 1.7 $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ *is a ring (the complex numbers). It is also a 2-dimensional vector space over* $\mathbb{R}$ *with basis* $\{1, i\}$.

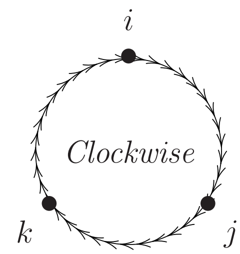
Example 1.8 *Consider a 4-dimensional vector space over* $\mathbb{R}$ *with basis* $\{1, i, j, k\}$. *We define multiplication as follows*

$$i^2 = j^2 = k^2 = -1 = ijk$$

$$ij = k \qquad ji = -k$$

$$jk = i \qquad kj = -i$$

$$ki = j \qquad ik = -j$$



$1.i = i.1 = i$, $1.j = j.1 = j$, $1.k = k.1 = k$ *and* $1.1 = 1$

Now define:

$$(a + bi + cj + dk)(e + fi + gj + hk) = (ae - bf - cg - dh) + (af + be + ch - dg)i$$
$$(ag + ce - bh + df)j + (ah + de + bg - cf)k$$

This multiplication gives us a non-commutative ring ($ij \neq ji$), called the Quaternions ($\mathbb{H}$).

Example 1.9 (***1840's Hamilton***) *Consider an n-dimensional vector space (over $\mathbb{R}$ say) with basis $\{e_1, e_2, \ldots, e_n\}$ (the basic units). Define the product $e_i.e_j \ \forall\ i, j = 1 \ldots n$. Then (as in the previous example) insist on the distributive laws and we see that this new object is a ring, called the set of* ***Hypercomplex Numbers*** *(M).*

Example 1.10 *If $\{e_1, e_2, \ldots, e_n\}$ forms a group (under multiplication) G, then the hypercomplex numbers generated by G is called the* ***Group Ring*** *($\mathbb{R}G$).* ***Arthur Cayley 1854****.*

Definition 1.11 *Given a group G and a ring R, define the* ***Group Ring*** *RG to be the set of all linear combinations*

$$\alpha = \sum_{g \in G} a_g g$$

where $a_g \in R$ and where only finitely many of the ${a_g}^s$ are non-zero.
Define the sum

$$\alpha + \beta = \left(\sum_{g \in G} a_g g \right) + \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} (a_g + b_g) g.$$

Define the product

$$\alpha\beta = \left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_h gh$$

Notes :

(1) We can also write the product $\alpha\beta$ as $\sum_{u\in G} C_u u$, where $C_u = \sum_{gh=u} a_g b_h$

(2) RG is a ring (with addition and multiplication defined as above).

(3) Given $\alpha \in RG$ and $\lambda \in R$, we can define a multiplication

$$\lambda.\alpha = \lambda \sum_{g\in G} a_g g = \sum_{g\in G} (\lambda a_g) g.$$

(4) RG is an example of a hypercomplex number system (if $R = \mathbb{R}$).

Definition 1.12 *Let R be a ring. An abelian group $(M, +)$ is called a **(left) R-module** if for each $a, b \in R$ and $m \in M$, we have a product $am \in M$ such that*

(i) $(a + b)m = am + bm$

(ii) $a(m_1 + m_2) = am_1 + am_2$

(iii) $a(bm) = (ab)m$

(iv) $1.m = m \ \forall\, a, b \in R$ *and* $\forall\, m, m_1, m_2 \in M$.

*Similarly we could define a **(right) R-module***

(i) $m(a + b) = ma + mb$

(ii) $(m_1 + m_2)a = m_1 a + am_2 a$

(iii) $m(ab) = (ma)b$

(iv) $m.1 = m \ \forall\, a, b \in R$ *and* $\forall\, m, m_1, m_2 \in M$.

If M is a left R-module and a right R-module, then we call M a ***(two-sided) R-module****.*

Definition 1.13 *Let R be a ring. An element $a \in R$ is* ***invertible*** *in R if $\exists\, b \in R$ such that $a.b = b.a = 1$.*

We write $b = a^{-1}$ (the inverse of a) and say that a is a **unit** of R.

Definition 1.14

$$\mathcal{U}(R) = \{a \in R \mid \textit{if } a \textit{ is a unit of } R\ \}$$

Note that $\mathcal{U}(R)$ is a group (with multiplication) called the **group of units** of R.

Example 1.15 $\mathcal{U}(\mathbb{Z}) = \{+1, -1\}$*, the cyclic group of order 2 (written C_2).*

Example 1.16 $\mathcal{U}(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$.

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \textit{ where } a \neq 0,\ b \neq 0$$

Example 1.17 $\mathcal{U}(\mathbb{R}) = \mathbb{R} \setminus \{0\}$.

Example 1.18 $\mathcal{U}(\mathbb{C}) = \mathbb{C} \setminus \{0\}$.

Example 1.19 $\mathcal{U}(\mathbb{H}) = \mathbb{H} \setminus \{0\}$.

Example 1.20 $\mathcal{U}(M_n(\mathbb{R})) = \{A \in M_n(\mathbb{R}) \mid det\, A \neq 0\} = GL_n(\mathbb{R})$.

Definition 1.21 *A ring R is called a* ***division ring*** *if every non-zero element of R is a unit. i.e. $\mathcal{U}(R) = R \setminus \{0\}$.*

Note : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$ are division rings. $\mathbb{Z}$ and $M_n(\mathbb{R})$ are not division rings.

Definition 1.22 *A division ring R is called a* ***(commutative) field*** *if R is a commutative ring.*

Note : $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields. $\mathbb{H}$ is not a field (non-commutative). $\mathbb{Z}$ is not a field (not a division ring).

Definition 1.23 $(\mathbb{Z}_n, +, \cdot)$ *is the ring of integers modulo* n (*where* $n \in \mathbb{Z}$, $n > 0$). *In fact this is a commutative ring.*

Example 1.24 *Consider* $(\mathbb{Z}_5, +, \cdot)$ *:* $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$ *and* $4^{-1} = 4$. *So* $\mathbb{Z}_5$ *is a division ring, so it is a field.*

Example 1.25 *Consider* $(\mathbb{Z}_6, +, \cdot)$ *:* $1^{-1} = 1$, 2^{-1} *doesn't exist,* 3^{-1} *doesn't exist,* 4^{-1} *doesn't exist and* $5^{-1} = 5$. *So* $\mathcal{U}(\mathbb{Z}_6) = \{1, 5\} =< 5 >\cong C_2$. *So* $\mathbb{Z}_6$ *is not a division ring and hence it is not a field.*

Definition 1.26 *In a ring* R, *if* $a.b = 0$ *but* $a \neq 0$ *and* $b \neq 0$ *then* a *and* b *are called* ***zero divisors***.

Definition 1.27 *If a ring* R *has no zero-divisors, then* R *is called an* ***integral domain*** (*or just a domain*).

Example 1.28 $(\mathbb{Z}, +, \cdot)$ *is an integral domain since* $a.b = 0 \Longrightarrow a = 0$ *or* $b = 0$.

Example 1.29 *In* $\mathbb{Z}_6$, *2.3=0. So 2 and 3 are zero divisors. Therefore* $\mathbb{Z}_6$ *is not an integral domain.*

Example 1.30 $(\mathbb{Z}_5, +, \cdot)$ *is an integral domain.*

Lemma 1.31 *Every division ring is an integral domain.*

Proof. We assume that R is a division ring. We want to show that R has no zero divisors. Proceed by contradiction : Assume $a.b = 0$, where $a \neq 0$ and $b \neq 0$. Since $0 \neq a \in R$ then we have $a^{-1} \in R$. $\therefore a^{-1}(ab) = a^{-1}(0) = 0 = (a^{-1}a)b = 1.b = b = 0$. This is a contradiction. ■

Notes :

(1) The converse is not true. i.e. there are integral domains which are not division rings. e.g. $(\mathbb{Z}, +, \cdot)$ is not an integral domain but not a division ring.

(2) Zero-divisors are never invertible.

Example 1.32 *Let* $R = \mathbb{F}_2 = \mathbb{Z}_2$ *and* $G = C_2$ ($\mathbb{Z}_2$ *is the ring of order 2, which is a field*). *Writing down the elements :* $\mathbb{F}_2 = \{0, 1\}$ *and* $C_2 = \{1, x\} =< x >=< x \,|\, x^2 = 1 >$.

$$
\begin{aligned}
\mathbb{F}_2C_2 &= \{\sum_{g\in C_2} a_g g \,|\, a_g \in \mathbb{F}_2\} \\
&= \{0_{\mathbb{F}_2}.1_{C_2} + 0_{\mathbb{F}_2}.x, 1_{\mathbb{F}_2}.1_{C_2} + 0_{\mathbb{F}_2}.x, 0_{\mathbb{F}_2}.1_{C_2} + 1_{\mathbb{F}_2}.x, 1_{\mathbb{F}_2}.1_{C_2} + 1_{\mathbb{F}_2}.x\} \\
&= \{0_{\mathbb{F}_2C_2}, 1_{\mathbb{F}_2C_2}, 1_{\mathbb{F}_2}.x, 1_{\mathbb{F}_2}.1_{C_2} + 1_{\mathbb{F}_2}.x\} \\
&= \{0, 1, x, 1+x\}
\end{aligned}
$$

Note that . is $\mathbb{F}_2$ module multiplication. Now let's construct the cayley tables for $\mathbb{F}_2C_2$.

$\underline{\mathbb{F}_2C_2}$

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0 $(\bullet)$	$1+x$	x
x	x	$1+x$	0 $(\star)$	1
$1+x$	$1+x$	x	1	0

$(\bullet)$ $1+1 = 1_{\mathbb{F}_2}.1_{C_2} + 1_{\mathbb{F}_2}.1_{C_2}$

$= (1_{\mathbb{F}_2} + 1_{\mathbb{F}_2})1_{C_2}$

$= (0_{\mathbb{F}_2})1_{C_2} = 0$

$(\star)$ $x + x = 1_{\mathbb{F}_2}.x + 1_{\mathbb{F}_2}.x$

$= (1_{\mathbb{F}_2} + 1_{\mathbb{F}_2})x$

$= (0_{\mathbb{F}_2})x = 0$

$(\mathbb{F}_2C_2, +)$ is a group.

$\underline{\mathbb{F}_2C_2}$

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	1	$1+x$
$1+x$	0	$1+x$	$1+x$	0 $(\bullet)$

$(\bullet)$ $(1+x)(1+x) = 1(1+x) + x(1+x)$

$= 1 + x + x + 1$

$= 2 + 2x = 0$

Clearly $(\mathbb{F}_2C_2, \cdot\,)$ is not a group (since $0.a = 0\ \forall\ a \in \mathbb{F}_2C_2$). Also $(\mathbb{F}_2C_2 \setminus \{0\}, \cdot\,)$ does not form a group (since $(1+x)^2 = 0$ and 0 is not an element of $\mathbb{F}_2C_2 \setminus \{0\}$.

Note : that the unit group of $\mathbb{F}_2C_2$ is $\{1, x\}$.

$\underline{\mathcal{U}(\mathbb{F}_2C_2)}$

$\mathcal{U}(\mathbb{F}_2C_2) = \{1, x\} \cong C_2$

$\cdot$	1	x
1	1	x
x	x	1

Conjecture 1.33 *$\mathcal{U}(RG) = G$.*

Note that G is isomorphic (as a group) to a subgroup of $\mathcal{U}(RG)$ via the embedding

$$\theta\ :\ G \hookrightarrow \mathcal{U}(RG) \quad g \mapsto 1.g$$

We often associate G with $\theta(G) < \mathcal{U}(RG)$ and abusing the notation, we write $G < \mathcal{U}(RG)$.

Recall that in $\mathbb{F}_2C_2$, $(1+x)^2 = 0$. So $1+x$ is the only zero divisor of $\mathbb{F}_2C_2$.

Conjecture 1.34 *$RG = \{0\} \cup \mathcal{U}(RG) \cup \mathcal{ZD}(RG)$ (where $\mathcal{ZD}(RG)$ are the zero divisors of G.*

Consider (1) $\mathbb{F}_3C_2$ and (2) $\mathbb{F}_2C_3$.

(1) $\mathbb{F}_3C_2$

$\mathbb{F}_3C_2 = \{a.1 + b.x \mid a, b \in \mathbb{F}_3\}$. There are 3 choices for $a \in \{0, 1, 2\}$ and there are 3 choices for $b \in \{0, 1, 2\}$ so there are $3.3 = 9$ elements in $\mathbb{F}_3C_2$.

(2) $\mathbb{F}_2C_3$

$C_3 = \{1, x, x^2\}$. $\mathbb{F}_2 C_3 = \{a.1 + b.x + c.x^2 \mid a, b, c \in \mathbb{F}_3\}$. There are 2 choices for $a \in \{0,1\}$, 2 choices for $b \in \{0,1\}$ and there are 2 choices for $c \in \{0,1\}$ so there are $2.2.2 = 8$ elements in $\mathbb{F}_2 C_3$.

Now $3 \leq |\mathbb{F}_2 C_3 \leq 8$ and $C_3 \lhd \mathcal{U}(\mathbb{F}_2 C_3)$. By Lagranges theorem $|c_3|$ divides $|\mathcal{U}(\mathbb{F}_2 C_3)|$ so $3 \mid |\mathcal{U}(\mathbb{F}_2 C_3)|$ and $|\mathcal{U}(\mathbb{F}_2 C_3)| \leq 8$, therefore $|\mathcal{U}(\mathbb{F}_2 C_3)| = 3$ or 6.

Lemma 1.35 *Let R be a ring of order m and G a group of order n. Then RG is a finite group ring of size $|R|^{|G|} = m^n$.*

Proof. $RG = \{\sum_{g \in G} a_g g \mid a_g \in R\}$. For each g, there are m choices for a_g. So there are $\underbrace{m.m \ldots m}_{|G|=n}$-elements in RG. i.e. $m^n = |R|^{|G|}$. ■

Example 1.36 $|\mathbb{F}_2 C_2| = |\mathbb{F}_2|^{|C_2|} = 2^2 = 4$. *The group $(\mathbb{F}_2 C_2, +)$ has order 4 so it is isomorphic to either C_4 or $C_2 \times C_2$. If $a \in \mathbb{F}_2 C_2$, then $2.a = 0.a = 0$. So every element of $\mathbb{F}_2 C_2$ has order ≤ 2. Thus $\mathbb{F}_2 C_2 \ncong C_4$ (since C_4 has an element of order 4). $\therefore$ $(\mathbb{F}_2 C_2, +) \cong C_2 \times C_2$ (Klein-4-group).*

Question : Is $\mathbb{F}_2 C_2 \cong \mathbb{Z}_4$ (isomorphic as rings) ? **Answer :** No. What is the additive group of $\mathbb{Z}_4$

$\underline{\mathbb{Z}_4}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

So $(\mathbb{Z}_2, +) \cong C_4$

Thus $\mathbb{F}_2 C_2$ and $\mathbb{Z}_4$ have non-isomorphic additive groups. So they are not isomorphic as rings.

1.2 Ring Homomorphisms and Ideals

Lemma 1.37 *Let $f : R \longrightarrow S$ be a ring homomorphism, then*

(i) $f(0_r) = 0_s$.

(ii) $f(-a) = -f(a)$.

Proof. **(i)** Take $a \in R$. $f(a) = f(a + 0_r) = f(a) + f(0_r)$. Thus $f(a) = f(a) + f(0) = f(0) + f(a)\ \forall\, a \in R$. So

$$\begin{aligned} -f(a) + f(a) &= 0_s \\ &= -f(a) + (f(a) + f(0_r)) \\ &= (-f(a) + f(a) + f(0_r) \\ &= 0_s + f(0_r) = f(0_r) \\ &= 0_s \end{aligned}$$

$$\therefore f(0_r) = 0_s$$

(ii) $f(a + (-a)) = f(0_r) = 0_s = f(a) + f(-a)$

$$\therefore f(-a) = -f(a)$$

. ■

Definition 1.38 *Let L be a subset of the ring R. L is called a* ***left ideal*** *of R if*

(i) $x, y \in L \Longrightarrow x - y \in L$.

(ii) $x \in L,\ a \in R \Longrightarrow ax \in L$ *(left multiplication by an element of R).*

$$\therefore R.L = L$$

Similarly we could define a right ideal of R. If L is a left ideal of R and a right ideal of R, we say that L is a **two-sided** ideal of R.

*** (used in the same way that normal subgroups are used in group theory). i.e. If $N \lhd G \Longrightarrow G \longrightarrow \dfrac{G}{N}$, $g \mapsto g.N$ is a group homomorphism with kernal N and image $\dfrac{G}{N}$, the factor group or quotient group of G by N.

$$\frac{G}{N} = \{gN \,:\, g \in G\}.$$

Recall : 1^{st}, 2^{nd} and 3^{rd} isomorphism theorems of groups.

Let I be an ideal of R. We write $I \lhd R$. Notice that I is a ring (usually without the multiplicative identity 1_r). $\Longrightarrow I$ is a subring of R.

Example 1.39 *Consider the ring $(\mathbb{Z}, +, \cdot)$. Let $n \in \mathbb{Z}$. Then $I = n\mathbb{Z} = \{n.a \,:\, a \in \mathbb{Z}\}$ is a (two sided) ideal of $\mathbb{Z}$, since*

$$\begin{aligned} na - nb = n(a-b) &\in n\mathbb{Z}\,\forall\, a, b \in \mathbb{Z} \\ c(n.a) = n(c.a) &\in n\mathbb{Z}\,\forall\, c \in \mathbb{Z} \end{aligned}$$

Example 1.40 *Consider the ring $(\mathbb{Z}_6, +, \cdot)$. What are the ideals of $(\mathbb{Z}_6, +, \cdot)$? Now consider the subset $I_2 = \{2.a \,:\, a \in \mathbb{Z}_6\} = \{0, 2, 4\}$. I_2 is an ideal of $\mathbb{Z}_6\}$ (exercise). $I_3 = \{3.a \,:\, a \in \mathbb{Z}_6\} = \{0, 3\}$ is an ideal of $\mathbb{Z}_6\}$ (exercise). $0 = \{0_{\mathbb{Z}_6}\} \lhd \mathbb{Z}_6\}$. Also $\mathbb{Z}_6 \unlhd \mathbb{Z}_6$. Note that $\mathbb{Z}_6\}$ is the only ideal of $\mathbb{Z}_6\}$ which contains $1_{\mathbb{Z}_6}$. Note : $I_1 = \{1.a \,:\, a \in \mathbb{Z}_6\} = \mathbb{Z}_6$. Are there any more ideals of $\mathbb{Z}_6$? Let I be an ideal of $\mathbb{Z}_6$. What is the size of I ?*

Lemma 1.41 (*Langrange theorem for rings*) *Let I be an ideal of a finite ring R. Then $|I| \,/\, |R|$.*

Proof. $(R, +)$ is a group, $(I, +)$ is a subgroup. Apply Lagranges theorem (for groups), we get $|I| \,/\, |R|$. ∎

Applying this lemma to the previous example, we see that $|I| = 1$, 2, 3 or 6. If $|I| = 1$, then $I = \{0_{\mathbb{Z}_6}\}$. If $|I| = 6$, then $I = \mathbb{Z}_6$. If $|I| = 2$, then $I = \{0, 3\}$. If $|I| = 3$, then $I = \{0, 2, 4\}$. Thus $\mathbb{Z}_6$ has 4 ideals.

Example 1.42 *Consider the ring* $(\mathbb{Z}_5, +, \cdot)$. *Let* $I_2 = \{2.a : a \in \mathbb{Z}_5\} = \{0, 2, 4, 1, 3\} = \mathbb{Z}_5$. *Therefore the only ideals of* $\mathbb{Z}_5$ *are* $\{0_{\mathbb{Z}_5}\}$ *and* $\mathbb{Z}_5$. *i.e. Let* $I \lhd \mathbb{Z}_5$, *then* $|I|/|\mathbb{Z}_5|$ *so* $|I| = 1$ *or* 5 *so* $I = \{0_{\mathbb{Z}_5}\}$ *or* $\mathbb{Z}_5$

Let $f : R \longrightarrow S$ be a ring homomorphism, then $f(1_r) = 1_s$ is not necessarily true.

Example 1.43 *Define* $f : M_2(\mathbb{Q}) \longrightarrow M_3(\mathbb{Q})$ *where* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}$.
Then $f\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ *and* f *is a ring homomorphism. However*
$f(I_2) = f\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq I_3$.

Note that here $f(A)f(I_2) = f(a.I_2) = f(A)$. So $f(I_2)$ seems to work like the multiplicative identity on the range of f.

Let $f : R \longrightarrow S$ be a ring homomorphism. Then $Ker(f) = \{x \in R : f(x) = 0\}$. If $x, y \in Ker(f)$, then $f(x + y) = f(x) + f(y) = 0 + 0 = 0$. Also $f(x - y) = f(x) - f(y) = 0 - 0 = 0$.

Let $x \in Ker(f)$, $s \in R$. Is $xs \in Ker(f)$? $f(xs) = f(x)f(s) = 0.f(s) = 0$. $\therefore xs \in Ker(f)$. So $Ker(f)$ is an ideal of R.

Definition 1.44 *A ring homomorphism* $f : R \longrightarrow S$ *is called*

(i) a ***monomorphism*** *(or embedding) if* f *is injective.*

(ii) an ***epimorphism*** *if* f *is surjective.*

Example 1.45 $\mathbb{Z} \overset{f}{\hookrightarrow} \mathbb{Q}$ *where* $f(n) = n$. $Ker(f) = \{0\} \subset \mathbb{Z}$.

Example 1.46 $\mathbb{Z} \overset{g}{\rightarrowtail} 2\mathbb{Z}$ *where* $g(n) = 2n$. $Ker(g) = \{0\} \subset \mathbb{Z}$.

Example 1.47 *Let* p *be a prime number. Define* $f : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ *by*
$f(n) = n + p\mathbb{Z}$.

$f(n+m) = n+m+p\mathbb{Z}$. $f(n)+f(m) = n+p\mathbb{Z}+m+p\mathbb{Z} = n+m+p\mathbb{Z}$. $\therefore f(n+m) = f(n)+f(m)$. Also $f(n-m) = f(n)-f(m)$.

$f(nm) = nm+p\mathbb{Z}$.

$$\begin{aligned} f(n)f(m) &= (n+p\mathbb{Z})(m+p\mathbb{Z}) \\ &= nm+np\mathbb{Z}+mp\mathbb{Z}+p^2\mathbb{Z}\mathbb{Z} \\ &= nm+p(n\mathbb{Z}+mp\mathbb{Z}+p\mathbb{Z}) \\ &= nm+p\mathbb{Z} \end{aligned}$$

Thus $f(nm) = f(n)f(m)$ and f is a ring homomorphism.

$Ker(f) = \{n \in \mathbb{Z} \,|\, f(n) = 0\} = \{n \in \mathbb{Z} \,|\, n+p\mathbb{Z} = 0_{\mathbb{Z}_p} = 0+p\mathbb{Z}\} = \{np \,|\, n \in \mathbb{Z}\}$

Since $f(np) = np+p\mathbb{Z} = p(n+\mathbb{Z}) = p\mathbb{Z} = 0+p\mathbb{Z} = 0$. So $f : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ has kernal $p\mathbb{Z}$.

Let $I \lhd R$. Then consider the set $R/I = \{I + r : r \in R\}$. Define

- addition by $(r+I)+(s+I) = (r+s)+I$.
- multiplication by $(r+I)(s+I) = (rs)+I$.

R/I is a ring (check i.e. $0_{R/I} = 0+I$, $(r+I)+(-r+I) = 0+I = 0_{R/I}$, and so on).

Consider the ring homomorphism $f : R \longrightarrow R/I$ defined by $f(r) = r+I$. What is $Ker(f)$? $Ker(f) = \{r \in R : f(r) = 0\} = \{r \in R : f(r) = 0+I\} = I$ (Since if $i \in I$, we have $f(i) = i+I = I$).

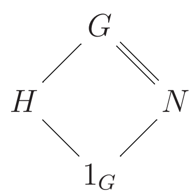
Therefore given any ideal I of a ring R, we can come up with a ring homomorphism $f : R \longrightarrow R/I$ such that $I = Ker(f)$. Note that we often write $f(r) = r+I = \overline{r}$ (r mod I).

Example 1.48 *$p\mathbb{Z} \lhd \mathbb{Z}$, $p\mathbb{Z}$ is the kernal of the homomorphism $f : \mathbb{Z} \longrightarrow \mathbb{Z}_p \cong \mathbb{Z}/\mathbb{Z}_p$.*

1.3 Isomorphism Theorems

Theorem 1.49 *(1^{st} Isomorphism theorem for groups) Let $f \rightarrowtail S$. Then $G/N \cong S$ where $N = Ker(f)$.*

For rings , the kernal is an ideal. Let G be a group, $H \lhd G$ and $N \unlhd G$. Then



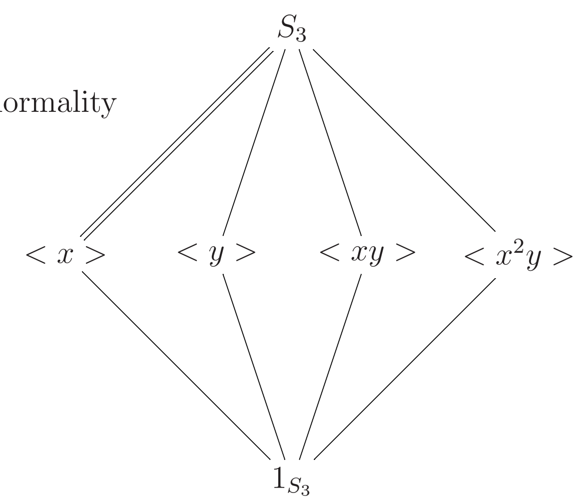
$$G/N \cong H/1$$

also

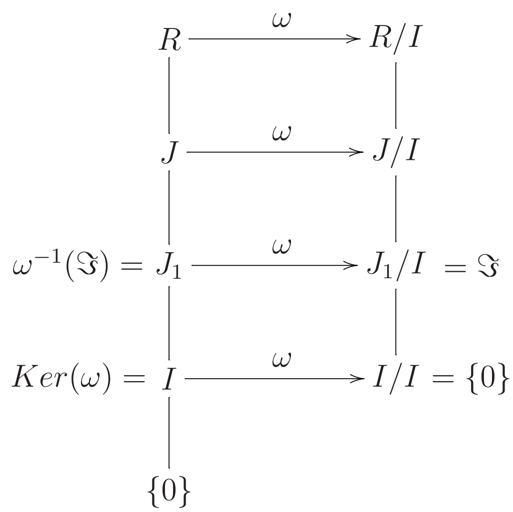
$$G/H \cong N/1$$

Example 1.50 $S_3 =< x, y \,|\, x^3 = y^2 = 1, yxy = x^2 >$. *Let's construct a lattice diagram of subgroups*

Double lines means normality

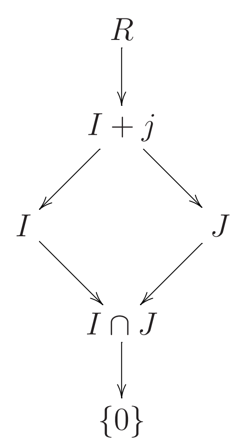


Now consider $\omega : R \longrightarrow R/I$ where $\omega(r) = r + I$ (the cononical projection). Let $J \supseteq I$, then $\omega(J) = \{j + I : j \in J\} = J/I \subset R/I$. J/I is not only a subset, it is also an ideal of R/I i.e. $J/I \lhd R/I$.



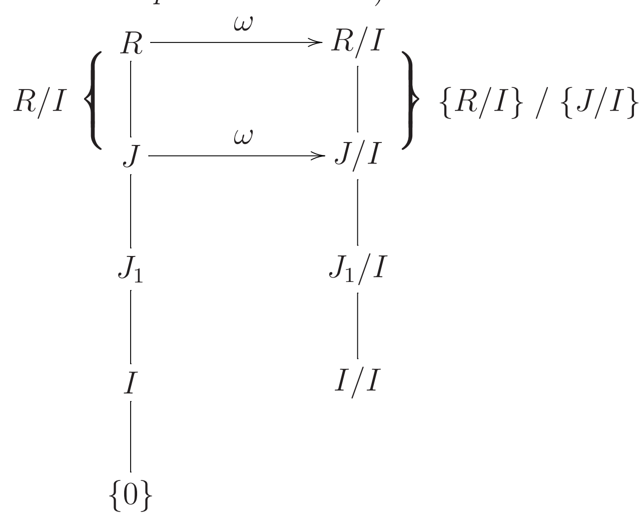
Note that a ring homomorphism preserves subsets and ideal.

Theorem 1.51 (2^{nd} *Isomorphism Theorem*)



$$\frac{I+J}{I} \cong \frac{J}{I \cap J} \quad also \quad \frac{I+J}{J} \cong \frac{I}{I \cap J}$$

Theorem 1.52 (3^{rd} *Isomorphism Theorem*)



Chapter 2

Ideals And Homomorphisms of RG

Let R be a ring (usually commuatative) and G a group. Then RG is a group ring (defined before). Since RG is a ring, we can talk about ideals of G, ring homomorphisms of RG and factor groups of RG.

Definition 2.1 *Consider the function* $\varepsilon : RG \longrightarrow R$ *defined by* $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$. *This function is called the* ***augmentation map****.* ε *maps* RG *onto* R*.*

Let $r \in R$ then $\varepsilon(r.1) = r$ (onto). Let $rg \in RG$ and $rh \in RG$, the $\varepsilon(rg) = \varepsilon(rh) = r$. However $rg \neq rh$, thus ε is not one-to-one. ε is a ring homomorphism from RG onto R (an epimorphism). Let $\alpha = \sum_{g\in G} a_g g$ and $\beta = \sum_{g\in G} b_g g$ where $\alpha, \beta \in RG$. Then

$$\varepsilon(\alpha+\beta) = \varepsilon\left(\sum_{g\in G}(a_g+b_g)g\right) = \sum_{g\in G}(a_g+b_g) = \sum_{g\in G} a_g + \sum_{g\in G} b_g = \varepsilon(\alpha)+\varepsilon(\beta)$$

Now let $\alpha = \left(\sum_{g\in G} a_g g\right)$ and $\beta = \left(\sum_{h\in G} b_h h\right)$.

$$\varepsilon(\alpha\beta) = \left(\sum_{g,h\in G} a_g b_h gh\right) = \sum_{g,h\in G} a_g b_h$$

$$\varepsilon(\alpha)\varepsilon(\beta) = \varepsilon\left(\sum_{g\in G} a_g g\right)\varepsilon\left(\sum_{h\in G} b_h h\right) = \left(\sum_{g\in G} a_g\right)\left(\sum_{h\in G} b_h\right) = \sum_{g,h\in G} a_g b_h$$

$\therefore \varepsilon(\alpha+\beta) = \varepsilon(\alpha)\varepsilon(\beta)$ and ε is a ring homomorphism.

$Ker(\varepsilon) = \{\alpha = \sum_{g\in G} a_g g \,|\, \varepsilon(\alpha) = \sum_{g\in G} a_g = 0\}$. $Ker(\varepsilon)$ is non empty and non trivial.

Example 2.2 *$rg + (-rh) \in Ker(\varepsilon)$ since $\varepsilon(rg + (-rh)) = r - r = 0$.*

Now $\dfrac{RG}{Ker(\varepsilon)} \cong R$. $Ker(\varepsilon)$ is an ideal called the **augmentation ideal** of RG and is denoted by $Ker(\varepsilon) = \Delta(RG)$.

Let $u \in \mathcal{U}(RG)$. Say $u.v = v.u = 1$. Then $\varepsilon(uv) = \varepsilon(1) = 1 = \varepsilon(u)\varepsilon(v) = 1 \in R$. So $\varepsilon(u)$ is invertible in R, with inverse $\varepsilon(v)$. So $\varepsilon(\mathcal{U}(RG)) \subset \mathcal{U}(R)$ i.e. ε sends units of RG to units of R.

Let $u \in \mathcal{ZD}(RG)$. Say $u.v = v.u = 0$ where $u, v \neq 0$. Then $\varepsilon(uv) = \varepsilon(u)\varepsilon(v) = \varepsilon(0) = 0$. Thus $\varepsilon(u)\varepsilon(v) = 0$. So either $\varepsilon(u) = 0$ or $\varepsilon(v) = 0$ or $\varepsilon(u)$ and $\varepsilon(v)$ are zero divisors in R.

If R has no zero divisors then this forces $\varepsilon(u) = 0$ or $\varepsilon(v) = 0$.

Example 2.3 *List all the elements of $\mathbb{F}_3C_2$, $\mathcal{U}(\mathbb{F}_3C_2)$ and $\mathcal{ZD}(\mathbb{F}_3C_2)$.*

$C_2 = \{1, x\}$ and $\mathbb{F}_3 = \{0, 1, 2\}.\mathbb{F}_3C_2 = \{a_1.1 + a_2.x \,|\, a_i \in \mathbb{F}_3\}$. Thus $|\mathbb{F}_3C_2| = 3.3 = 3^2 = 9$ $(|\mathbb{F}_3|^{|C_2|})$.

Writing the elements in lexicographical order :

$$0+0.x,\ 0+1.x,\ 0+2.x$$
$$1+0.x,\ 1+1.x,\ 1+2.x$$
$$2+0.x,\ 2+1.x,\ 2+2.x$$

$\mathbb{F}_3C_2 = \{0, 1, 2, x, 2x, 1+x, 1+2x, 2+x, 2+2x\}$.

$$\varepsilon : \mathbb{F}_3C_2 \longrightarrow \mathbb{F}_3$$

$\varepsilon(\alpha)$	$\alpha \in \mathbb{F}_3C_2$
0	$\{0, 2+x, 1+2x\}$
1	$\{1, x, 2+2x\}$
2	$\{2, 2x, 1+x\}$

$\mathcal{U}(\mathbb{F}_3C_2) = \{1, x, 2, 2x\}$, since $1^2 = 1$, , $x^2 = 1$, $2^2 = 1$ and $(2x)^2 = 1$. In a group inverses are unique, so we don't need to multiply these anymore. $\mathcal{U}(\mathbb{F}_3C_2) \cong C_2 \times C_2$ since it has no elements of order 4, so $\mathcal{U}(\mathbb{F}_3C_2) \ncong C_4$.

$(1+x)(1+x) = 1+x+x+x^2 = 2+2x \neq 1$. $(1+x)(2+x) = 2+x+2x+x^2 = 0 \neq 1$. Note that these are zero divisors so they are not units. Also $(1+2x)(1+2x) = 1+2x+2x+4x^2 = 2+x$ and $(1+2x)(2+2x) = 2+2x+4x+4x^2 = 0$.

$$\therefore \mathcal{ZD}(\mathbb{F}_3C_2)\{1+x, 2+x, 1+2x, 2+2x\}$$

Note $\mathbb{F}_3C_2) = \mathcal{U}(\mathbb{F}_3C_2) \cup \mathcal{ZD}(\mathbb{F}_3C_2) \cup \{0\}$.

Conjecture 2.4 *In general in any group ring RG, do we have*

$$\mathbb{F}_3C_2) = \mathcal{U}(\mathbb{F}_3C_2) \cup \mathcal{ZD}(\mathbb{F}_3C_2) \cup \{0\}$$

Lemma 2.5 *Let I be an ideal of a ring R, with $I \neq R$. Then I contains no invertible elements.*

Proof. Suppose $u \in I$, with u invertible (say $u.v = v.u = 1$). Now since I is an ideal, we have $v.i \in I \ \forall \ i \in I$. In particular, $v.u = 1 \in I$. If r is any element of R, then $r.1 \in I$. So $R \subset I$. So $R = I$ contradiction. ■

Lemma 2.6 *Let D be a division ring. Then*

- *(i) D has no ideals (apart from $\{0\}$ and itself).*
- *(ii) D has no zero divisors (done before !).*

Proof. (i) Let $I \lhd D$, with $I \neq \{0\}$. Let $x \neq 0$ and $x \in I$. So $0 \neq x \in D$, so x is invertible, by the previous lemma $I = D$.

(ii) Let $u.v = 0$ with $u \neq 0$ and $v \neq 0$ (and $u, v \in D$). Now u^{-1} and v^{-1} exists so $u^{-1}(uv) = u^{-1}.0 \Longrightarrow v = 0$, which is a contradiction. ■

Definition 2.7 *An elementary matrix $E_{i,j}$ is the matrix of all whose entries are) except for the $(i,j)^{th}$ entry which is 1.*

Example 2.8

$$E_{1,2} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Lemma 2.9 *Let D be a division ring and $R = M_n(D)$ ($n \times n$ matrices over division ring D). Then $M_n(D)$ has no ideals (apart from $\{0\}$ and $M_n(D)$).*

Proof. If $n = 1$, then this just part (i) of the above lemma. Let $B_i = E_{i,h}AE_{k,i}$. Now all entries of B_i equal) except for the $(i,i)^{\text{th}}$, which is $a_{h,k}$. Thus $B_i = a_{h,k}E_{i,i} \ \forall \ i \in \{1, 2, \dots, n\}$. Now I was a (two sided) ideal, $A \in I$

and $B_i = E_{i,h}AE_{k,i}$ so $B_i \in I$. (Now add up all the ideals). Let

$$\begin{aligned} B &= B_1 + B_2 + \cdots + B_n \\ &= a_{h,k}\{E_{1,1} + E_{2,2} + \cdots + E_{n,n}\} \\ &= a_{h,k}\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}. \end{aligned}$$

Thus B is invertible and $B \in I$. Thus (by the secind last lemma)

$$I = M_n(D)$$

■

Definition 2.10 *Let R_1 and R_2 be rings. Define a new ring, the **direct sum** of R_1 and R_2 as*

$$R_1 \oplus R_2 = \{(r_1, r_2) \,|\, r_1 \in R_1,\ r_2 \in R_2\} \quad (= \underbrace{R_1 \times R_2}_{\text{cartesian product}})$$

Let (r_1, r_2) and $(s_1, s_2) \in R_1 \oplus R_2$. Define $(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$ and $(r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$. This defines a ring (check!).

$R_1 \oplus R_2$ is not a division ring since for any non-zero $r \in R_1$ and $sinR_2$, we have $(r, 0)(0, s) = (r.0, 0.s) = (0, 0) = 0 \in R_1 \oplus R_2$. So $(r, 0)$ and $(0, s)$ are zero divisors. So $(r, 0)$ and $(0, s)$ are not invertible. So Hamilton would not be pleased. We could define $(R_1 \oplus R_2) \oplus R_3 = R_1 \oplus R_2 \oplus R_3$ and $\dots$ and $R_1 \oplus R_2 \oplus \dots \oplus R_3$.

Definition 2.11 *A ring R is called a **simple ring** if it's only ideals are $\{0\}$ and R (i.e. no non-trivial ideals).*

Note : $M_n(D)$ is a simple ring.

Definition 2.12 *An element $e \in R$ is called an **idempotent** if $e^2 = e$.*

Example 2.13 *In* $\mathbb{Z}_6$*, 3 is an idempotent since* $3^2 = 9 = 3$*.*

Example 2.14 *In* $M_2(\mathbb{F}_2)$*,* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ *and* $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ *are idempotents since*

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Definition 2.15 *The* ***center*** *of* R *is*

$$Z(R) = \{z \in R \,|\, zr = rz \;\forall\, r \in R\}$$

Question : Is $Z(R)$ a ring ?
Question : Is $Z(R)$ an ideal ?

Definition 2.16 e *is called a* ***central idempotent*** *if* $e^2 = e$ *and* $e \in Z(R)$*.*

Definition 2.17 *A ring* R *is* ***semisimple*** *if it can be decomposed as a direct sum of finitely many minimal left ideals. i.e.* $R = L_1 \oplus \cdots \oplus L_t$*, where* L_i *is a minimal left ideal.*

Note : L is a minimal left ideal of R if L is a left ideal of R ($L \overset{l}{\lhd} R$) and if J is any other left ideal of R contained in L, then either $J = \{0\}$ or $J = L$.

Example 2.18 $M_n(D)$ *is a semisimple ring. Let* $L_1 = \begin{pmatrix} D & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$

and let $L_2 = \begin{pmatrix} 0 & D & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$ *and ... let* $L_n = \begin{pmatrix} 0 & 0 & 0 & \dots & D \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$.
For each i*,* L_i *is a minimal left ideal of* R *(check!). Also* $M_n(D) = L_1 \oplus \cdots \oplus L_n$ *so* $M_n(D)$ *is semisimple (check!).*

Lemma 2.19 *Let R be s ring. R is semisimple iff every left ideal of R is a direct summand of R.*

Example 2.20 *In the above example $L_1 \oplus L_2$ is a left ideal of R and $(L_1 \oplus L_2) \oplus (L_3 \cdots \oplus L_n) = R$.*

Theorem 2.21 *Let R be a ring. R is semisimple iff every left ideal of R is of the form $L = Re$, where $e \in R$ is an idempotent.*

Proof. $(\Rightarrow)$ Assume that R is semisimple. Let $L \overset{l}{\lhd} R$. By the previous lemma, L is a direct summand of R. So there exists a left ideal $L' \overset{l}{\lhd} R$ such that $L \oplus L' = R$. So $1 = x + y$ for some $x \in L$ and $y \in L'$. (**Question :** Is this decomposition unique ?).
Then $x = x.1 = x(x+y) = x^2+xy$ So $\underbrace{xy}_{\in L'} = \underbrace{x - x^2}_{\in L}$. Thus $xy \in L \cap L' = \{0\}$.
Thus $xy = 0 = x - x^2$, so $x = x^2$. Hence, x is an idempotent. We have shown $L = Rx$ where $x \in L$ so $Rx \subset L$. We must show $L \subset Rx$. Let $a \in L$. Then $a = a.1 = a(x + y) = ax + ay = a$. $\therefore \underbrace{a - ax}_{L} = \underbrace{ay}_{L'} \in L \cap L' = \{0\}$. So $a - ax = 0$ so $a = ax \in Rx$. Thus $L \subset Rx$. So $L = Rx$.

$(\Leftarrow)$ assume that every left ideal of R is of the form $L = Re$ for some idempotent $e \in R$. We will show that every left ideal is a direct summand of R. Let $L \overset{l}{\lhd} R$. Then $L = Re$. Let $L' = R(1 - e)$. Then L' is a left ideal of R. (Note $(1 - e)^2 = 1 - e - e + e^2 = 1 - 2e + e = 1 - e$). We must show that $L \oplus L; = R$ (i.e. $L + L' = R$ and $L \cap L' = \{0\}$).

Let $x \in R$ Then $x = x.1 = x(e + (1 - e)) = xe + x(1 - e) \in L + L'$. $\therefore R = L \oplus L'$. Let $x \in L \cap L' = Re \cap R(1 - e)$. Then $x = r.e = s(1 - e)$, $r, s \in R$. Thus $x.e = (r.e).e = r.e^2 = r.e = x$. Also $x.e = (s(1 - e))e = s(e - e^2) = s(0) = 0$. Thus $x = 0$ so $L \cap L' = \{0\}$ and so $R = L \oplus L'$. ■

Let $\alpha = \sum_{g \in G} a_g g \in RG$. Now all but finitely many of the a_g's are non-zero. We define the **support of** α as

$$\operatorname{supp} \alpha = \{g \in G \mid a_g \neq 0\}$$

The group $< \operatorname{supp} \alpha >$ (generated by the support of α) is a finitely generated group. So $R < \operatorname{supp} \alpha > \subset RG$.

Proposition 2.22 *The set $\{g-1 \,|\, g \in G,\, g \neq 1\}$ is a basis for $\Delta(G)$ over R.*

i.e. $\Delta(G) = \{\sum_{g\in G} a_g(g-1) \,|\, g \in G,\, g \neq 1\}$ and the $g-1$ are linearly independant over R.

Proof. Let $\alpha = \sum_{g\in G} a_g g \in \Delta(G)$. So $\sum_{g\in G} a_g = 0$. Thus $\alpha = \sum_{g\in G} a_g g - 0 = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1)$ so this is a spanning set for $\Delta(G)$. We will show linear independance :

Let $\sum_{g\in G} a_g(g-1) = 0$. Then $0 = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g g = 0 \Longleftrightarrow a_g = 0\ \forall\ g \in G$. Since G is linear independant over R, by the definition of the group ring RG.

■

Note : RG has dimension $|G|$ over R. $\Delta(G)$ has dimension $|G|-1$ over R. If R is a field then these are vector spaces. Otherwise they are R-modules.

Proposition 2.23 *Let R be a commutative ring. The map*

$$* : RG \longrightarrow RG \quad \textit{where} \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g g^{-1}$$

is an ***involution****. Then $*$ has the following properties :*

(i) $(\alpha+\beta)^* = \alpha^* + \beta^*$

(ii) $(\alpha\beta)^* = \alpha^*\beta^*$

(iii) $(\alpha^*)^* = \alpha$

Proof. Homework 2. ■

Proposition 2.24 *Let $I \lhd R$ and let G be a group. Then*

$$IG = \{\sum_{g\in G} a_g g \,|\, a_g \in I\} \lhd RG$$

Also

$$\frac{RG}{IG} \cong \left(\frac{R}{I}\right) G.$$

Proof. (a) IG is a commutative group under $+ \checkmark$. Let $\alpha = \sum_{g \in G} a_g g \in IG$ and $\beta = \sum_{h \in G} b_h h \in RG$ (so $a_g \in I$ and $b_h \in R$ forall $g, h \in G$).

$$\alpha\beta = \left(\sum_{g \in G} a_g g\right)\left(\sum_{h \in G} b_h h\right) = \sum_{g,h \in G} \underbrace{a_g b_h}_{\in I} gh \in IG$$

So IG is an ideal of RG.

(b) $\frac{RG}{IG} = \{\beta + IG \mid \beta \in RG\}$ and $\left(\frac{R}{I}\right) G = \{\sum_{g \in G}(a_g + I)g \mid a_g + I \in \frac{R}{I}\}$. i.e. $a_g \in R$ and $g \in G$. Define

$$\theta : \frac{RG}{IG} \longrightarrow \left(\frac{R}{I}\right) G$$

by $\theta(\beta + IG) = \theta\left(\sum_{g \in G} b_g g + IG\right) = \sum_{g \in G}(b_g + I)G$. We must show that θ is an isomorphism.

$\theta(\alpha + IG + \beta + IG) = \theta(\alpha + \beta + IG) = \theta(\sum(a_g + b_g + IG) = \sum(a_g + b_g + I)g$.
Also $\theta(\alpha + IG) + \theta(\beta + IG) = \sum(b_g + I)g + \sum(a_g + I)g = \sum(a_g + b_g + I)g$ $\checkmark$.
$\theta((\alpha + IG)(\beta + IG)) = \theta(\alpha\beta + IG) = \theta(\sum_{g \in G} a_g g \sum_{h \in G} b_h h + IG) = \sum_{g,h \in G}(a_g b_h + I)gh$.
Also $\theta(\alpha + IG)\theta(\beta + IG) = (\sum(a_g + I)g)(\sum(b_h + I)h) = \sum(a_g + I)(b_h + I)gh = \sum(a_g b_h + I)gh$ $\checkmark$. $\therefore \theta$ is a ring homomorphism. It remains to show that θ is bijective but we will do this on homework 2. ∎

Chapter 3

Group Ring Representations

Definition 3.1 *Let G be a finite group and R a ring. The R-module RG (the group ring RG) with the natural multiplication $g\alpha$ $(g \in G,\ \alpha \in RG)$. Now given $g \in G$, g acts on the basis of RG by left multiplication and permutes the basis elements. Define $\mathcal{T} : G \longrightarrow GL_n(R)$ where $g \mapsto \mathcal{T}_g$ and $\mathcal{T}_g$ acts on the basis elements by left multiplication. So if $G = \{g_1 = 1, g_2, \ldots, g_n\}$ and $\mathcal{T}_g\ g_i = gg_i \in G$. The function $\mathcal{T}$ from G to $GL_n(R)$ is called the (left-regular)* ***group representation*** *of the finite group G over the ring R.*

Think of $\mathcal{T}_g$ as left multiplication by a group element or left multiplication of a column vector by a $n \times n$ matrix.

Lemma 3.2 *Let G be a finite group of order n. Let R be a ring. Then the group representation $\mathcal{T}$ is an injective homomorphism (monomorphism) from G to $GL_n(R)$.*

Proof. Let $g, h \in G$ and $g_i \in G$ where g_i are the basis elements. We want to show $\mathcal{T}(gh) = \mathcal{T}(g)\mathcal{T}(h)$. Now $\mathcal{T}(gh).(g_i) = (gh).g_i = g(hg_i) = \mathcal{T}_g(\mathcal{T}_h(g_i))\ \forall g_i \in G = \mathcal{T}(g)\mathcal{T}(h)(g_i)$. $\therefore \mathcal{T}(gh) = \mathcal{T}(g)\mathcal{T}(h)$.

1-1 : We must show that if $\mathcal{T}(g) = I_n \in GL_n(R) \Longrightarrow g = 1_G$. Let $g \in G$ with $\mathcal{T}(g) = I_n$. Then $\mathcal{T}(g)(g_i) = g_i\ \forall g_i \in G$. In particular (with $g_i = g_1 = 1_G$), $\mathcal{T}(g)(1) = I_n \Longrightarrow g.1 = 1 \Longrightarrow g = 1$. ■

Example 3.3 *Let $G = C_3 =< a \,|\, a^3 = 1 >$.*

$\therefore RG = \{\lambda_1.1 + \lambda_2.a + \lambda_3.a^2 \,|\, \lambda_i \in R\}$. What does $g.\alpha$ look like (where $g \in G$ and $\alpha \in RG$) ?

$$\begin{aligned} 1(\lambda_1.1 + \lambda_2.a + \lambda_3.a^2) &= \lambda_1.1 + \lambda_2.a + \lambda_3.a^2 \\ (*)\ a(\lambda_1.1 + \lambda_2.a + \lambda_3.a^2) &= \lambda_3.1 + \lambda_1.a + \lambda_2.a^2 \\ (**)\ a^2(\lambda_1.1 + \lambda_2.a + \lambda_3.a^2) &= \lambda_2.1 + \lambda_3.a + \lambda_1.a^2 \end{aligned}$$

Correspondance

$$1 \longleftrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},\ a \longleftrightarrow \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},\ a^2 \longleftrightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

(these are the basis elements which are acted upon, permuted by left-multiplication by 3×3 matrices).

$\mathcal{T} : 1 \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$,

$a \longrightarrow \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ from $(*)\ a(\lambda_1.1+\lambda_2.a+\lambda_3.a^2) \longleftrightarrow a \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \begin{pmatrix} \lambda_3 \\ \lambda_1 \\ \lambda_2 \end{pmatrix}$,

$a^2 \longrightarrow \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ from $(**)\ a^2(\lambda_1.1 + \lambda_2.a + \lambda_3.a^2) \longleftrightarrow a^2 \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \begin{pmatrix} \lambda_2 \\ \lambda_3 \\ \lambda_1 \end{pmatrix}$.

Note

$$\begin{aligned} & a(\lambda_1.1 + \lambda_2.a + \lambda_3.a^2) \\ \longleftrightarrow & \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \left(\begin{pmatrix} \lambda_1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \lambda_2 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \lambda_3 \end{pmatrix} \right) \\ = & \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \begin{pmatrix} \lambda_3 \\ \lambda_1 \\ \lambda_2 \end{pmatrix} \\ \longleftrightarrow & \lambda_3.1 + \lambda_1.a + \lambda_2.a^2) \end{aligned}$$

We can extend the definition of a left regular group representation to a left regular group ring representation as follows :

Let R be a commutative ring and G a finite group. Define

$$\mathcal{T} : RG \longrightarrow M_n(R), \quad \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g \mathcal{T}_g$$

where $\mathcal{T}_g$ acts on the basis $G = \{g_1 = 1, g_2, \dots, g_n\}$ by left multiplication (i.e. $\mathcal{T}_g(g_i) = gg_i$.

Lemma 3.4 *$\mathcal{T}$ above is a ring (write $\mathcal{T}_\alpha = \mathcal{T}(\alpha)$) homomorphism from the group ring RG to the set of $n \times n$ matrices over R. Also $\mathcal{T}(r\alpha) = r\mathcal{T}(\alpha)\ \forall\ r \in R$, $\forall\ \alpha \in RG$. Also if R is a field then $\mathcal{T} : RG \longrightarrow M_n(R)$ is injective.*

Proof. Homework 2. ■

If R is commutative then define

- det(α) =det($\mathcal{T}(\alpha)$)
- tr(α) =tr($\mathcal{T}(\alpha)$)
- eigenvalue of (α) = eigenvalue of ($\mathcal{T}(\alpha)$)
- eigenvectors of (α) = eigenvectors of ($\mathcal{T}(\alpha)$) where $\alpha \in RG$.

Lemma 3.5 *Let K be a field and G a finite group.*

(*i*) *If $\alpha \in KG$ is nilpotent (i.e. $\exists m \in N$ such that $\alpha^m = 0$), then the eigenvalues of $(\mathcal{T}(\alpha))$ are all zero.*

(*ii*) *If $\beta \in KG$ is a unit of finite order (i.e. $\exists n \in N$ such that $\beta^n = 1$), then the eigenvalues of $(\mathcal{T}(\alpha))$ are all n^{th} roots of unity.*

(*iii*) *If $f(\gamma) = 0$, $\exists\, \gamma \in KG$ and $\exists\, f \in K[x]$ (the set of all polynomials over K) then $f(\lambda_i) = 0\ \forall$ eigenvalues λ_i of $(\mathcal{T}(\gamma))$*

Proof. Note that $(iii) \Longrightarrow (i)$ and (ii). **(i)** Let $\alpha \in KG$ with $\alpha^m = 0$. Let λ be an eigenvalue of $(\mathcal{T}(\alpha))$ i.e. $(\mathcal{T}(\alpha))X = \lambda X$ where X is a $n \times 1$ column vector with entries in K. Now $(\mathcal{T}(\alpha))^m.X = \lambda^m.X$. $(\mathcal{T}(\alpha))^m.X = \mathcal{T}(\alpha)^m.X = \mathcal{T}(0).X = 0_{n\times n}X = 0_{n\times 1}$ since $\mathcal{T}$ is a ring homomorphism.
$\therefore \lambda^m.X = 0_{n\times 1} \Longrightarrow \lambda^m = 0_{n\times 1}$ (since K has no zero divisors) $\Longrightarrow \lambda = 0$.

(ii) Let $\beta \in KG$ with $\beta^n = 1$. Let λ be an eigenvalue of $(\mathcal{T}(\beta))$ i.e. $(\mathcal{T}(\beta))X = \lambda X$. Now $(\mathcal{T}(\beta))^n.X = \lambda^n.X$. $(\mathcal{T}(\beta))^n.X = \mathcal{T}(\beta^n).X = \mathcal{T}(1).X = I_{n\times n}.X = X$. $\therefore \lambda^n.X = X \Longrightarrow \lambda^n = 1$ (since K is a field) $\Longrightarrow \lambda$ is an $\mathrm{n^{th}}$ root of unity.

(iii) Let $f(\gamma) = 0\ \forall\ \gamma \in KG$ and $\exists\, f \in K[x]$. Let λ be an eigenvalue of $(\mathcal{T}(\gamma))\therefore (\mathcal{T}(\gamma))X = \lambda X. \Longrightarrow f(\mathcal{T}(\gamma)).X = f(\lambda).X$ since $\mathcal{T}$ is a $K-linear$ ring homomorphism on RG. $f(\mathcal{T}(\gamma)).X = \mathcal{T}(f(\gamma)).X = \mathcal{T}(0).X = 0.X = 0$.
$\therefore f(\lambda).X = 0 \Longrightarrow f(\lambda) = 0$. ■

Example 3.6 *Let R be a ring and let G be a finite group. We define the* ***trivial group*** *representation of G as :*

$$\mathcal{T} : G \longrightarrow GL_n(R) \qquad g \mapsto I_{n\times n} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

$\mathcal{T}(gh) = I_{n\times n}$. $\mathcal{T}(g)\mathcal{T}(h) = I_{n\times n}.I_{n\times n} = I_{n\times n}$. So $\mathcal{T} : G \longrightarrow \{I_{n\times n}\} \cong C_1$ is a group epimorphism.

We now extend $\mathcal{T}$ to a group ring representation. $\mathcal{T} : RG \longrightarrow M_n(R)$ where

$$\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g \mathcal{T}(g) = \sum_{g\in G}(a_g I_{n\times n}) = (\sum_{g\in G} a_g)I_{n\times n} = \varepsilon\left(\sum_{g\in G} a_g g\right) I_{n\times n}$$

Example 3.7 *Let $2g + (-2h) \in RG$. Then $\mathcal{T}(2g + (-2h))$*

$$= \varepsilon(2g+(-2h))I_{n\times n} = (2+-2)I_{n\times n} = 0I_{n\times n} = 0_{n\times n} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Example 3.8 *Let $2g + (-2h) + 21 \in RG$. Then $\mathcal{T}(2g + (-2h) = 21)$*

$$= \varepsilon(2g+(-2h)+21)I_{n\times n} = (2+-2+21)I_{n\times n} = 21I_{n\times n} = \begin{pmatrix} 21 & 0 & 0 & \dots & 0 \\ 0 & 21 & 0 & \dots & 0 \\ 0 & 0 & 21 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 21 \end{pmatrix}.$$

Note $\mathcal{T} : RG \longrightarrow M_n(R)$ is onto and the $Ker(\mathcal{T}) = \Delta(RG)$.

Lemma 3.9 *Let G be a finite group and K a field. Let $\mathcal{T}$ be the left regular representation of KG and let $\gamma = \sum_{g\in G} c_g g \in KG$. Then the trace of $\mathcal{T}(\gamma)$ is*

$$tr(\,\mathcal{T}(\gamma)\,) = |G|.c_1$$

(where c_1 is the coefficient of $g_1 = 1$. For example if $\gamma = 2 + 3g + 4h \in KG$, then $c_1 = 2$).

Proof. The traces of similar matrices are the same and so $\mathrm{tr}\,(\,\mathcal{T}(\gamma)\,)$ is independant of choice of basis. Fix the basis $G = \{g_1 = 1, g_2, \dots, g_n\}$ (a K-basis of KG). $\therefore \mathcal{T}(\gamma) = \mathcal{T}\left(\sum_{g\in G} c_g g\right) = \sum_{g\in G} c_g \mathcal{T}(g) = \sum_{i=1}^{n} c_{g_i}\mathcal{T}(g_i)$. If $g \neq 1$, then $gg_i \neq g_i\ \forall\ i$ so g permutes the basis of KG.

So the matrix of $\mathcal{T}(g)$ has all zero's in it's main diagonal. Hence the $\operatorname{tr}(\mathcal{T}(g)) = 0 \;\forall\, g \in G$ except for $g = 1$.

$$
\begin{aligned}
\therefore \operatorname{tr}(\mathcal{T}(\gamma)) &= \operatorname{tr}\left(\sum_{i=1}^{n} c_{g_i} g_i\right) \\
&= \sum_{i=1}^{n} c_{g_i} \operatorname{tr}(\mathcal{T}(g_i)) \\
&= c_{g_1}\operatorname{tr}(\mathcal{T}(g_1)) + c_{g_2}\operatorname{tr}(\mathcal{T}(g_2)) + \cdots + c_{g_n}\operatorname{tr}(\mathcal{T}(g_n)) \\
&= c_{g_1}\operatorname{tr}\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} + 0 + \cdots + 0 \\
&= c_{g_1}.|G| \\
&= c_1.|G|
\end{aligned}
$$

■

Theorem 3.10 (***Berman-Higman***) *Let $\gamma = \sum_{g \in G} c_g g$ be a unit of finite order in $\mathbb{Z}G$, where G is a finite group and $c_1 \neq 0$. Then $\gamma = \pm 1 = c_1$.*

Proof. Let $|G| = n$ and let $\gamma^m = 1$. Considering $\mathbb{Z}G$ as a subring of $\mathbb{C}G$, we will consider it's left regular representation and apply the previous lemma. Then $\operatorname{tr}(\mathcal{T}(\gamma)) = n.c_1$. Now $\gamma^m = 1$ therefore all the eigenvalues of $\mathcal{T}(\gamma)$ are the n^{th} roots of unity.

$$\therefore \operatorname{tr}(\mathcal{T}(\gamma)) = \operatorname{tr}(\mathcal{T}\left(\sum_{i=1}^{n} c_{g_i} g_i\right)) = \sum c_g \operatorname{tr}(\mathcal{T}(g)) = \sum(\text{eigenvalue of } \operatorname{tr}(\mathcal{T}(\gamma)))$$

Now $\mathcal{T}(\gamma)$ is similar to a diagonal matrix D ($\mathcal{T}(\gamma) \backsim D$). So $\operatorname{tr}(\mathcal{T}(\gamma)) = \operatorname{tr} D$ $= \sum$ diagonal elements of $D = \sum$ eigenvalues of $D = \sum$ eigenvalue of $\mathcal{T}(\gamma)$

$= \sum_{i=1}^{n} \eta_i$ where η_i is an n$^{\text{th}}$ roots of unity.

$$\begin{aligned}
\therefore nc_1 &= \sum_{i=1}^{n} \eta_i \\
\therefore |nc_1| &= |\sum_{i=1}^{n} \eta_i| \leq \sum_{i=1}^{n} |\eta_i| = n. \\
\therefore |c_1| &\leq 1 \Longrightarrow c_1 = \pm 1 \\
\therefore nc_1 &= \sum_{i=1}^{n} \eta_i = n \text{ or} - n, \text{ so } \eta_i = \eta_i \; \forall \; i \\
\text{so } nc_1 &= n\eta_i \Longrightarrow \eta_i = \pm 1 \; \forall \; i \\
\therefore \mathcal{T}(\gamma) &\backsim D = I \text{ or } I \\
\therefore \mathcal{T}(\gamma) &= I \text{ or } I
\end{aligned}$$

But $\mathcal{T} : \mathbb{C}G \longrightarrow M_n(\mathbb{C})$ is injective, so $\gamma = \pm 1 \; (= c_1)$. ■

Corollary 3.11 *Let $\gamma \in Z(\mathcal{U}(\mathbb{Z}G))$ where $\gamma^m = 1$ and G is finite. Then $\gamma = \pm g \, \exists \, g \in G$. (i.e. all central torsion units are trivial).*

Proof. Let $\gamma \in Z(\mathcal{U}(\mathbb{Z}G))$ with $\gamma^m = 1$ and $|G| = n$. Let $\gamma = \sum_{i=1}^{n} c_{g_i} g_i$ and let $c_{g_2} \neq 0 \, \exists \, g_2 \in G$. $\therefore \gamma {g_2}^{-1} = \sum_{i=1}^{n} c_{g_i} g_i {g_2}^{-1} \, (\star)$ is a unit of finite order in $\mathbb{Z}G$ (Let ${g_2}^{m_2} = 1$, then $(\gamma {g_2}^{-1})^{m.m_2} = \gamma^{m.m_2} ({g_2}^{-1})^{m.m_2} = 1.1 = 1$ since γ is central).

Now from $(\star)$ the coefficient of 1 in $\gamma {g_2}^{-1}$ is $c_{g_2} \neq 0$. Now applying the Berman-Higman theorem to $\gamma {g_2}^{-1}$ to get that

$$\gamma {g_2}^{-1} = \pm 1 = c_{g_2} \Longrightarrow \gamma = \pm 1.g_2 = \pm g_2 \; \exists \; g_2 \in G$$

■

Theorem 3.12 (***Higman***) *Let A be a finite abelian group. Then the group of torsion units of $\mathbb{Z}A$ equals $\pm A$.*

Example 3.13 *What are the torsion units of* $\mathbb{Z}C_3$ *? Just* $\pm C_3$.

If $C_3 =< x \,|\, x^3 = 1 >= \{1, x, x^2, \}$, then the torsion units of $\mathbb{Z}C_3$ are $\pm C_3 = \{1, x, x^2, -1, -x, -x^2\} \cong C_3 \times C_2 =< x > \times < -1 >\cong C_6 \cong< -x >$.

Question : Are the torsion units of RG equals $\pm G$ or $\mathcal{U}(R).G$ for all groups G and rings R ?

Chapter 4

Decomposition of RG

Theorem 4.1 *Let R be a semisimple ring with*

$$R = \oplus_{i=1}^{t} L_i$$

where the L_i are minimal left ideals. Then $\exists\, e_1, e_2, \ldots, e_n \in R$ such that

(i) $e \neq 0$ *is an idempotent for* $i = 1, \ldots, t$.

(ii) *If* $i \neq j$, *then* $e_i e_j = 0$.

(iii) $e_1 + e_2 + \cdots + e_t = 1$.

(iv) e_i *cannot be written as* $e_i = e_i' + e_i''$ *(where* e_i' *and* e_i'' *are idempotents such that* $e_i' e_i'' = 0 = e_i'' e_i'$ *).*

Conversely, if $\exists\, e_1, e_2, \ldots, e_t \in R$ satisfying the four conditions above, then the left ideals $L_i = Re_i$ are minimal and $R = \oplus_{i=1}^{t} L_i$ (and $\therefore R$ is semisimple).
Proof. ($\Rightarrow$). Let $R = \oplus_{i=1}^{t} L_i$, where L_i is a minimal left ideal (for $i = \{1, 2, \ldots, t\}$).

(iii) $1 \in R$, so $1 = e_1 + e_2 + \cdots + e_t \;\exists\, e_i \in L_i$.

(i) Indeed, $e_i = 1.e_i = (e_1 + e_2 + \cdots + e_t)e_i = e_1 e_i + e_2 e_i + \cdots + {e_i}^2 + \cdots + e_t$.
$\Longrightarrow \underbrace{e_i - {e_i}^2}_{\in L_i} = \underbrace{e_1 e_i + e_2 e_i + \cdots + e_{i-1} e_i + e_{i+1} e_i + \cdots + e_t}_{L_1 \oplus L_2 \oplus \cdots \oplus L_{i-1} \oplus L_{i+1} \oplus \cdots \oplus L_t}$.
$\therefore e_i - {e_i}^2 \in L_1 \oplus L_2 \oplus \cdots \oplus L_{i-1} \oplus L_{i+1} \oplus \cdots \oplus L_t \Longrightarrow e_i - {e_i}^2 = 0 \Longrightarrow e_i = {e_i}^2$.

(ii) $e_i = (0, \ldots, 0, 1.e_i, 0, \ldots, 0) \in L_1 \oplus \cdots \oplus L_t$. $\therefore e_i e_j =$
$(0, \ldots, 0, 1.e_i, 0, \ldots, 0)(0, \ldots, 0, 1.e_j, 0, \ldots, 0) = (0, \ldots, 0) = 0$.

(iv) Assume that (iv) does not hold, so $e_i = e_i' + e_i''$, (where e_i' and e_i'' are idempotents such that $e_i'e_i'' = 0 = e_i''e_i'$). Note that $R = \oplus_{i=1}^t L_i = \oplus_{i=1}^t Re_i$. $Re_i \subset L_i$ since $e_i \in L_i$ and L_i is a left ideal. Show $L_i \subset Re_i$. Let $a \in L_i$. Then $a = a.1 = a(e_1 + e_2 + \cdots + e_t) = ae_1 + ae_2 + \cdots + ae_t$.

$$\Longrightarrow \underbrace{a - ae_i}_{\in L_i} = \underbrace{ae_1 + ae_2 + \cdots + ae_{i-1} + ae_{i+1} + \cdots + ae_t}_{L_1 \oplus L_2 \oplus \cdots \oplus L_{i-1} \oplus L_{i+1} \oplus \cdots \oplus L_t}.$$

$\therefore a - ae_i = 0 \Longrightarrow a = ae_i \in Re_i$ and so $Re_i = l_i$.
$L_i = Re_i = R(e_i' + e_i'') = Re_i' \oplus Re_i''$. Now Re_i' and Re_i'' are left ideal so L_i is not minimal. This is a contradiction.

($\Leftarrow$) skip. ■

Note : A set of idempotents $\{e_1, e_2, \ldots, e_t\}$ with properties (i),(ii) and (iii) above are called **complete family of orthogonal idempotents**. If $\{e_1, e_2, \ldots, e_t\}$ has the property of (i)-(iv), then it is called a set of **primitive idempotents**.

Theorem 4.2 (***Wedderburn-Artin Theorem***) *R is a semisimple ring if and only if R can be decomposed as a direct sum of finitely many matrix rings over division rings.*

$$i.e.\ R \cong M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \cdots \oplus M_{n_s}(D_s)$$

where D_i is a division ring and $M_{n_i}(D_i)$ is the ring of $n_i \times n_i$ matrices over D_i.

Theorem 4.3 *Let R be a semisimple ring. Then the wedderburn-artin decomposition above is unique.*

$$i.e.\ R \cong \oplus_{i=1}^s M_{n_i}(D_i) \cong \oplus_{i=1}^t M_{m_i}(D_{i'}) \Longrightarrow s = t$$

and after permuting indices $n_i = m_i$ and $D_i = D_{i'}$ $\forall\ i \in 1, \ldots, s$.

Theorem 4.4 (***Maschke's Theorem***) *Let G be a group and R a ring. Then RG is semisimple if the following conditions hold :*

(i) R is semisimple

(ii) G is finite

(iii) $|G|$ is invertible in R.

Corollary 4.5 *Let G be a group and K a field. Then KG is semisimple if and only if G is finite and the characteristic $K \nmid |G|$.*

Proof. First note that any field K is semisimple ($K = M_1(K)$ and use a previous lemma).
($\Leftarrow$) Let $|G| < \infty$ and char$K \nmid |G|$. So $|G| \in K \setminus \{0\}$.
($\Rightarrow$) $|G|$ is invertible in K. Now apply maschke's theorem $\Longrightarrow$ let KG be semisimple. G is finite by maschke's and also $|G|$ is invertible in K so $|G| \in K \setminus \{0\}$. So $|G|$ is not a multiple of char $K \in K$. $\therefore K \nmid |G|$. ■

Theorem 4.6 *Let G be a finite group and K a finite field such that char $K \nmid |G|$. Then $KG \cong \oplus_{i=1}^{s} M_{n_i}(D_i)$ where D_i is a division ring containing K in it's center and*

$$|G| = \sum_{i=1}^{s} ({n_i}^2 . dim_K(D_i))$$

Definition 4.7 *A field K is* ***algebraically closed*** *if it contains all of the roots of the polynomials in $K[x]$.*

Example 4.8 *$\mathbb{C}$ is algebraically closed, while $\mathbb{H}$ is not.*

Corollary 4.9 *Let G be a finite group and K an algebraically closed field, where char $K \nmid |G|$. Then*

$$KG \cong \oplus_{i=1}^{s} M_{n_i}(K) \quad \textit{and} \quad |G| = \sum_{i=1}^{s} {n_i}^2$$

Example 4.10 *$\mathbb{C}C_3$. Note that C_3 is finite and char $\mathbb{C} = 0 \nmid 3$ so maschke's theorem does apply and*

$$\mathbb{C}C_3 \cong \oplus_{i=1}^{s} M_{n_i}(D_i) = \oplus_{i=1}^{s} M_{n_i}(\mathbb{C}) \ \textit{ by the corollary above}$$

Counting dimensions we see that $3 = \sum_{i=1}^{s} {n_i}^2 = \sum_{i=1}^{3} 1^2$. $\therefore D_i = \mathbb{C},\ n_i = 1\ \forall\ i$ *and* $s = 3$. $\therefore \mathbb{C}C_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$. $\therefore \mathcal{U}(\mathbb{C}C_3) \cong \mathcal{U}(\mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}) = \mathcal{U}(\mathbb{C}) \times \mathcal{U}(\mathbb{C}) \times \mathcal{U}(\mathbb{C})$.

The zero divisors of $\mathbb{C}C_3$ *correspond bijectively to the zero divisors of* $\mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$

$$= \{(a, b, 0) \,|\, a, b \in \mathbb{C}\} \cup \{(a, 0, c) \,|\, a, c \in \mathbb{C}\} \cup \{(0, b, c) \,|\, b, c \in \mathbb{C}\}$$

Example 4.11 $\mathbb{C}S_3$. S_3 *is finite and* $\mathbb{C} = 0 \nmid 6$ *so maschke's theorem does apply and*

$$\mathbb{C}S_3 \cong \oplus_{i=1}^{s} M_{n_i}(D_i) = \oplus_{i=1}^{s} M_{n_i}(\mathbb{C})$$

$6 = 1^2 + 1^2 + 2^2$ *or* $6 = \sum_{i=1}^{6} 1^2$. *So* $\mathbb{C}S_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$ *or* $\mathbb{C}S_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$. *But* $\oplus_{i=1}^{6}\mathbb{C}$ *is a commutative ring so* $\mathbb{C}S_3 \ncong \oplus_{i=1}^{6}\mathbb{C}$.

$\therefore \mathbb{C}S_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$ *and* $\therefore \mathcal{U}(\mathbb{C}S_3) \cong \mathcal{U}(\mathbb{C}) \times \mathcal{U}(\mathbb{C}) \times GL_2(\mathbb{C})$. *The zero divisors of* $\mathbb{C}S_3$ *correspond bijectively to the zero divisors of* $\mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$.

$$\begin{aligned} &= \{(a, b, A) \,|\, a, b, \in \mathbb{C},\ A \in \mathcal{ZD}(M_2(\mathbb{C}))\} \\ &= \{(a, 0, A) \,|\, a, \in \mathbb{C},\ A \in \mathcal{ZD}(M_2(\mathbb{C}))\} \cup \{(0, b, A) \,|\, b, \in \mathbb{C},\ A \in \mathcal{ZD}(M_2(\mathbb{C}))\} \end{aligned}$$

Example 4.12 $\mathbb{F}_2C_2$ *does not compose as* $\oplus_{i=1}^{s} M_{n_i}(D_i)$ *since* $2|2$ (*i.e char* $\mathbb{F}_2 \,|\, |G|$).

Theorem 4.13 (***Wedderburn***) *A finite division ring is a field.*

Example 4.14 $\mathbb{F}_3C_2$. *Maschke's theorem applies since* $|C_2| < \infty$ *and char* $\mathbb{F}_3 \nmid |C_2|$. $\therefore \mathbb{F}_3C_2 \cong \oplus_{i=1}^{s} M_{n_i}(D_i)$. $2 = \sum_{i=1}^{s} ({n_i}^2.\ dim_{\mathbb{F}_3}(D_i))$. *Note that* $\mathbb{F}_3$ *is not algebraically closed (check). So we need* $dim_{\mathbb{F}_3}(D_i)$. *Now* $2 = 1 + 1 = 1.2$. *So* $dim_{\mathbb{F}_3}(D) = 1$ *or* 2. $\therefore \mathbb{F}_3C_2 \cong \mathbb{F}_3 \oplus \mathbb{F}_3$ *or* $\therefore \mathbb{F}_3C_2 \cong D$ *where* $dim_{\mathbb{F}_3}(D) = 2$.

$$\therefore \mathbb{F}_3C_2 \cong \mathbb{F}_3 \oplus \mathbb{F}_3 \text{ or } \mathbb{F}_{3^2}$$

Question : Which one is it ?

Theorem 4.15 *The unit group of any finite field $\mathbb{F}_{p^n}$ (with p a prime) is cyclic of order $p^n - 1$. So $\mathcal{U}(\mathbb{F}_{p^n}) \cong C_{p^n-1}$. So any element of $\mathbb{F}_{p^n}$ has (multiplicative) order dividing $p^n - 1$.*

Example 4.16 *Consider $\mathbb{F}_5$. $1 = 1$. $2^2 = 4$, $2^3 = 3$, $2^4 = 1$. $3^2 = 4$, $3^3 = 2$, $3^4 = 1$. $4^2 = 1$. Therefore the elements of $\mathcal{U}(\mathbb{F}_5)$ have order $1, 4, 4, 2$. These all divide $5 - 1 = 4$.*

Thus $\mathcal{U}(\mathbb{F}_3 C_2) \cong \mathcal{U}(\mathbb{F}_3) \times \mathcal{U}(\mathbb{F}_3) = C_2 \times C_2$ or $\mathcal{U}(\mathbb{F}_3 C_2) \cong \mathcal{U}(\mathbb{F}_{3^2}) = C_{3^2-1} = C_8$. However (by homework 1) $\mathcal{U}(\mathbb{F}_3 C_2) \cong C_2 \times C_2$. So $\mathbb{F}_3 C_2 \not\cong \mathbb{F}_{3^2}$ so

$$\mathbb{F}_3 C_2 \cong \mathbb{F}_3 \oplus \mathbb{F}_3$$

(Alternatively, note that $\mathcal{U}(\mathbb{F}_3 C_2)$ and $\mathbb{F}_3 \oplus \mathbb{F}_3$ contain zero divisors but $\mathbb{F}_{3^2}$ does not).

Theorem 4.17 *Let G be a finite group and K a field such that char $K \nmid |G|$. Then*

$$KG \cong \oplus_{i=1}^{s} M_{n_i}(D_i) \cong K \oplus \oplus_{i=1}^{s-1} M_{n_i}(D_i)$$

(i.e. the field itself appears at least once as a direct summand in the Wedderburn-Artin decomposition).

Proof. Later ■

Lemma 4.18 *Let K be a finite field. Then if char $K \nmid |G| < \infty$, then*

$$KG \cong \oplus_{i=1}^{s} M_{n_i}(K_i)$$

where the K_i are fields (i.e. all the division rings appearing are fields).

Proof. Clearly $KG \cong \oplus_{i=1}^{s} M_{n_i}(D_i)$ where the D_i are division rings. But D_i is a division ring such that $dim_K D_i < \infty$ (since G is finite). Now Wedderburn's theorem implies that D_i must be a field. ■

Example 4.19 *Consider $\mathbb{F}_5 S_3$. $\mathbb{F}_5 S_3 \cong \oplus_{i=1}^{s} Mn_i(D_i) \cong \mathbb{F}_5 \oplus \oplus_{i=1}^{s-1} M_{n_i}(D_i) \cong \mathbb{F}_5 \oplus \oplus_{i=1}^{s-1} M_{n_i}(K_i)$.*

$\therefore \oplus_{i=1}^{s-1} M_{n_i}(K_i)$ *is a 5-dimensional vectors space over* $\mathbb{F}_5$*. But* $\mathbb{F}_5 S_3$ *is non-commutative so* $n_i > 1 \ \exists \ i$*.*

$$\therefore \oplus_{i=1}^{s-1} M_{n_i}(K_i) = \mathbb{F}_5 \oplus M_2(\mathbb{F}_5)$$

$$\therefore \mathbb{F}_5 S_3 \cong \oplus_{i=1}^{s} Mn_i(K_i) \cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus M_2(\mathbb{F}_5)$$

$$\therefore \mathcal{U}(\mathbb{F}_5 S_3) \cong \mathcal{U}(\mathbb{F}_5) \times \mathcal{U}(\mathbb{F}_5) \times \mathcal{U}(M_2(\mathbb{F}_5)) \cong C_4 \times C_4 \times GL_2(\mathbb{F}_5)$$

$GL_2(\mathbb{F}_5) = \{A \in M_2(\mathbb{F}_5) \mid det\ A = 0\} = \{A \in M_2(\mathbb{F}_5) \mid$ *rows of* A *are linearly independant.*
Check : $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \dfrac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$*. Now let's count the size of* $GL_2(\mathbb{F}_5)$*:*

There are $5^2 - 1 = 24$ *choices for the first row (not including the zero row) and there are* $5^2 - 5 = 20$ *choices for the second row (not a multiple of the first row).* $\therefore |GL_2(\mathbb{F}_5)| = (5^2 - 1)(5^2 - 5) = 480$*.* $\therefore \mathcal{U}(\mathbb{F}_5 S_3)$ *has order* $4.4.480 = 7680$*.*

Theorem 4.20 $GL_2(\mathbb{F}_p)$ *is a non abelian group of order* $(p^2 - 1)(p^2 - p)$*.* $GL_2(\mathbb{F}_{p^n})$ *is a non abelian group of order* $(p^{2n} - 1)(p^{2n} - p^n)$*.* $GL_3(\mathbb{F}_{p^n})$ *is a non abelian group of order ? (Homework).*

Definition 4.21 *Let* $x \in G$ *be an element of order* n *(i.e.* $x^n = 1$*). Then define*

$$\widehat{x} = 1 + x + x^2 + \cdots + x^{n-1} \in RG$$

Definition 4.22 *Let* $H < G$ *(H-finite so* $H = \{h_1, h_2, \ldots, h_n\}$*). Then define*

$$\widehat{H} = h_1 + h_2 + \cdots + h_n \in RH \subset RG.$$

So $\widehat{x} =< x >\in \ R < x > \subset RG$.

Lemma 4.23 *Let* H *be a finite subgroup of* G *and* R *any ring (with unity). If* $|H|$ *is invertible in* R *then* $e_H = \dfrac{1}{|H|}.\widehat{H} \in RH$ *is an idempotent. Moreover if* $H \lhd G$ *then* $e_H = \dfrac{1}{|H|}.\widehat{H}$ *is central in* RG*.*

Proof. **(i)** $H < G$.

$$\begin{aligned} {e_H}^2 &= \frac{1}{|H|}.\widehat{H}\frac{1}{|H|}.\widehat{H} \\ &= \frac{1}{|H|^2}\sum_{i=1}^{n} h_i\widehat{H} \quad \text{where } |H| = n. \\ &= \frac{1}{|H|^2}\sum_{i=1}^{n}\widehat{H} \\ &= \frac{1}{|H|^2}.n.\widehat{H} \\ &= \frac{1}{|H|^2}.|H|.\widehat{H} \\ &= \frac{1}{|H|}.\widehat{H} = e_H \end{aligned}$$

(ii) Let $H \lhd G$. We will show that e_H commutes with every element of RG. It suffices to show that e_H commutes with every element of G. So we must show that ${e_H}^g = g^{-1}e_H g = e_H \ \forall\ g \in G$. Now ${e_H}^g = g^{-1}\frac{1}{|H|}.\widehat{H}g$ $= \frac{1}{|H|}g^{-1}(h_1 + h_2 + \cdots + h_n)g = \frac{1}{|H|}(h_1 + h_2 + \cdots + h_n) = e_H$. ■

Definition 4.24 *Let X be a subset of RG. Then the* ***left-annihilator*** *of X in RG is*

$$ann_l(X) = \{\alpha \in RG \,|\, \alpha.x = 0 \ \forall\ x \in X\}$$

Similarly we can define the ***right-annihilator*** *of X in RG is*

$$ann_r(X) = \{\alpha \in RG \,|\, x.\alpha = 0 \ \forall\ x \in X\}$$

Definition 4.25 $\Delta_R(G,H) = \{\sum_{h\in H}\alpha_h(h-1) \,|\, \alpha_h \in RG\}$ *We usually write* $\Delta_R(G,H) = \Delta(G,H)$.

Note : $\Delta(G,H) \overset{l}{\lhd} RG$ (left ideal, check).
Note : $\Delta(G,G) = \Delta(G)$.

Lemma 4.26 *Let $H < G$ and R a ring. Then $\mathcal{A}nn_r(\Delta(G,H)) \neq 0$ iff H is finite. In this case*

$$\mathcal{A}nn_l(\Delta(G,H)) = \widehat{H}.RG.$$

Furthermore, if $H \lhd G$ then $\widehat{H}$ is central in RG and

$$\mathcal{A}nn_r(\Delta(G,H)) = \mathcal{A}nn_l(\Delta(G,H)) = \widehat{H}.RG = RG.\widehat{H}$$

Proof. ($\Rightarrow$). Let's assume that $\mathcal{A}nn_r(\Delta(G,H)) \neq 0$ and let $0 \neq \alpha = \sum a_g g \in \mathcal{A}nn_r(\Delta(G,H))$. So if $h \in H$ we get $(h-1)\alpha = 0$ (since $h - 1 \in \Delta(G,H)$).

$\Longrightarrow h\alpha = \alpha$, so $\sum a_g g = \sum a_g h_g$. Let $g_0 \in \operatorname{supp}\alpha$, so $\alpha_{g_0} \neq 0$. So $hg_0 \in \operatorname{supp}\alpha \ \forall\, h \in H$. But $\operatorname{supp}\alpha$ is finite so H is finite.

($\Leftarrow$). Conversely, let H be finite. $\therefore\ \widehat{H}$ exists and $\widehat{H} \in \mathcal{A}nn_r(\Delta(G,H))$. $\therefore\ \mathcal{A}nn_r(\Delta(G,H)) \neq 0$.

" In this case ... " : Assume that $\mathcal{A}nn_r(\Delta(G,H)) \neq 0$ i.e. H is finite. Let $0 \neq \alpha = \sum a_g g \in \mathcal{A}nn_r(\Delta(G,H))$. As before $\alpha_{g_0} = \alpha_{hg_0}$.

Now we can partition G into it's cosets (generated by H) to get

$$\begin{aligned}
\alpha &= \sum a_g g \\
&= a_{g_0}\widehat{H}g_0 + a_{g_1}\widehat{H}g_1 + \cdots + a_{g_t}\widehat{H}g_t \\
&= \widehat{H}\left(\sum_{i=1}^{t} a_{g_i} g_i\right) \\
&= \widehat{H}B \ \exists\ B \in RG \\
\therefore &\quad \mathcal{A}nn_r(\Delta(G,H)) \subset \widehat{H}.RG.
\end{aligned}$$

Clearly $\widehat{H}.RG \subset \mathcal{A}nn_r(\Delta(G,H))$ (since $(h-1)\widehat{H}RG = 0.RG = 0$).
"Furthermore ..." easy. ■

Proposition 4.27 *Let R be a ring and $H \lhd G$. If $|H|$ is invertible in R then letting $e_H = \frac{1}{|H|}.\widehat{H}$ we have*

$$RG \cong RG.e_H \oplus RG(1 - e_H)$$

where $RG.e_H \cong R(G/H)$ and $RG(1 - e_H) \cong \Delta(G,H)$.

Proof. e_H is a central idempotent. By the Pierce decomposition

$$RG \cong RG.e_H \oplus RG(1-e_H)$$

Now show $RG.e_H \cong R(G/H)$. Consider $\phi : G \longrightarrow Ge_H$ where $g \mapsto ge_H$. This is a group epimorphism since $\phi(gh) = ghe_h = ghe_H{}^2 = ge_H he_H = \phi(g)\phi(h)$. $Ker\,\phi = \{g \in G \,|\, ge_H = e_H\} = \{g \in G \,|\, ge_H - e_H = 0\} = \{g \in G \,|\, (g-1)e_H = 0\} = H$ since $(g-1)\frac{1}{|H|}\widehat{H} = 0 \Longrightarrow g\widehat{H} = \widehat{H}$.

$$\therefore \frac{G}{Ker\phi} = \frac{G}{H} \cong Im\,\phi = Ge_H$$

(by the 1^{st} Isomorphism Theorem of Groups). Now Ge_H is a basis of the group ring RGe_H so $RG.e_H \cong R(G/H)$.

Now show $RG(1-e_H) \cong \Delta(G,H)$. $RG(1-e_H) = \{\alpha \in RG \,|\, \alpha RGe_H = 0\}$ $= ann(RGe_H)$. Clearly, $\Delta(G,H) \subset ann(RGe_H)$ since $\sum_{h\in H} \alpha_h(1-h)RGe_H$ $= \sum_{h\in H} \alpha_h(1-h)\frac{1}{|H|}.\widehat{H}RG = 0$. It remains to show that $ann(RGe_H) \subset \Delta(G,H)$ (skip). ∎

Corollary 4.28 *Let R be a ring and G a finite group with $|G|$ invertible in R. Then*

$$RG \cong R \oplus \Delta(G).$$

Proof. Let $H = G \lhd G$ in the previous proposition.

$$\begin{aligned} \therefore RG &\cong R(G/G) \oplus \Delta(G,G) \\ &\cong R\{1\} \oplus \Delta(G) \\ &\cong R \oplus \Delta(G). \end{aligned}$$

∎

Lemma 4.29 *Let $H < G$ and S a set of generators of H. Then $\{s-1 \,|\, s \in S\}$ is a set of generators of $\Delta(G,H)$, as a left ideal of RG.*

Proof. Let $H =< s >$. Let $1 \neq h \in H \therefore h = {s_1}^{\varepsilon_1}{s_2}^{\varepsilon_2}\ldots{s_r}^{\varepsilon_r}$, where $s_i \in S$ and $\varepsilon_i = \pm 1$. Recall

$$\Delta_R(G, H) = \{\sum_{h \in H} \alpha_h(h-1) \,|\, \alpha_h \in RG\}.$$

So we must show that $h \in H \Longrightarrow h-1 \in RG\{s-1 \,|\, s \in S\}$. Now $h - 1 = {s_1}^{\varepsilon_1}\ldots{s_r}^{\varepsilon_r} - 1 = ({s_1}^{\varepsilon_1}\ldots{s_{r-1}}^{\varepsilon_{r-1}})({s_r}^{\varepsilon_r} - 1) + ({s_1}^{\varepsilon_1}\ldots{s_{r-1}}^{\varepsilon_{r-1}} - 1)$.

If $\varepsilon_r = 1$ then we are done (by induction on r). If $\varepsilon_r = -1$, then use $s_r^{-1} - 1 = s_r^{-1}(1 - s_r) = -s_r^{-1}(s_r - 1)$ and $h - 1 \in RG\{s-1 \,|\, s \in S\}$.

Note : we used $x^{-1} - 1 - x^{-1}(1-x)$ and $xy - 1 = x(y-1) + (x-1)$ and induction on r. ■

Recall : If $N \lhd G$ then G/N is commutative if and only if $G' < N$.

Lemma 4.30 *Let R be a commutative ring and I an ideal of RG. Then RG/I is commutative if and only if $\Delta(G, G') \subset I$.*

Proof. Let $I \lhd RG$, R commutative. ($\Rightarrow$). RG/I commutative $\Longrightarrow \forall\, g, h \in G$ we have $gh - hg \in I$. $gh = hg = hg(g^{-1}h^{-1}gh - 1) = hg([h, g] - 1) \in I$. $\Longrightarrow [h, g] - 1 \in I$. $\therefore \Delta(G, G') \subset I$ (by the previous lemma).

($\Leftarrow$). Assume $\Delta(G, G') \subset I$. Then $gh - hg = hg([h, g] - 1) \in \Delta(G, G') \subset I$. $\therefore gh = hg \bmod \Delta(G, G')$, so g and h commute modulo I so RG/I is commutative. ■

Proposition 4.31 *Let G be finite. Let RG be semisimple (i.e. $RG \cong \oplus_{i=1}^{s} M_{n_i}(D_i)$). Let $e_{G'} = \frac{1}{|G'|}.\widehat{G'}$. Then*

$$RG \cong RGe_{G'} \oplus RG(1 - e_{G'}) \cong R(G/G') \oplus \Delta(G, G').$$

Here $R(G/G')$ is the direct sum of all the commutative summands of the decomposition of RG and $\Delta(G, G')$ is the direct sum of all the non-commutative summands of the decomposition of RG.

Proof. Clearly $RG \cong R(G/G') \oplus \Delta(G, G')$. Now it is also clear that $R(G/G') \cong \oplus$ sum of the commutative summands of RG. It suffices to show that $\Delta(G, G')$ contains no commutative summands.

Assume $\Delta(G, G') \cong A \oplus B$ where A is commutative (and $\neq \{0\}$). Thus $RG \cong R(G/G') \oplus A \oplus B$. Now $RG/B \cong R(G/G') \oplus A$ (check). (In general, $R \cong C \oplus D \Longrightarrow R/C \cong D$). So RG/B is commutative, so by the previous lemma , $\Delta(G, G') \subset B$. Thus $\Delta(G, G') \cong A \oplus B \subset B$ which is a cotradiction. ∎

Definition 4.32 *$D_{2n} =< x, y \,|\, x^n = y^2 = 1, yxy = x^{-1} >$ is called the **dihedral group** of order $2n$.*

Note : $D_{2.3} = D_6 \cong S_3$.

Example 4.33 *$\mathbb{F}_3 D_{10}$. Note that Maschke applies so $\mathbb{F}_3 D_{10} \cong \oplus_{i=1}^{s} M_{n_i}(D_i)$ $\cong \oplus_{i=1}^{s} M_{n_i}(K_i)$ (where K_i are finite fields containing $\mathbb{F}_3$) $\mathbb{F}_3 \oplus \oplus_{i=1}^{t} M_{n_i}(K_i)$*

Note : *$D_{10} =< x, y \,|\, x^5 = y^2 = 1, yxy = x^4 >$. $\therefore [x, y] = x^{-1}y^{-1}xy = x^4yxy = x^4.x^4 = x^8 = x^3$. $\therefore D_{10}{}' >< x^3 >$ so $D_{10}{}' >< x >\cong C_5$.*

$\therefore \mathbb{F}_3 D_{10} \cong \mathbb{F}_3(D_{10}/D_{10}{}')\oplus$ non-commutative piece $\cong \mathbb{F}_3 C_2 \oplus$ non-commutative piece $\cong \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus$ non-commutative piece. By counting dimensions we get either

$$\mathbb{F}_3 D_{10} \cong \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus M_2(\mathbb{F}_3) \oplus M_2(\mathbb{F}_3)$$

or

$$\mathbb{F}_3 D_{10} \cong \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus M_2(\mathbb{F}_{3^2})$$

Example 4.34 *$\mathbb{F}_5 D_{12}$. $5 \nmid 12$ so maschke applies. $\mathbb{F}_5 D_{12} \cong \oplus_{i=1}^{s} M_{n_i}(D_i) \cong$*

$\mathbb{F}_5 \oplus_{i=1}^{s-1} M_{n_i}(K_i).D_{12} =< x, y \,|\, x^6 = y^2 = 1,\, yxy = x^5 >.$ ${D_{12}}' =$ *?*

$$\begin{aligned}
[x^iy^j, x^ky^l] &= y^{-j}x^{-i}y^{-l}x^{-k}x^iy^jx^ky^l \quad i,k \in \{0,1,2,3,4,5\}\ j,l \in \{0,1\} \\
&= y^jx^{-i}y^lx^{-k}x^iy^jx^ky^l \\
&= x^{(-i)(-1)j}y^{j+l}x^{i-k}y^jx^ky^l \\
&= x^{(-i)j(-1)}x^{(i-k)(-1)(j+l)}y^{j+j+l}x^ky^l \\
&= x^{(-i)j(-1)+(i-k)(-1)(j+l)}x^{k(-1)(2j+l)}y^{2j+2l} \\
&= x^{(-i)j(-1)+(i-k)(-1)(j+l)+k(-1)(2j+l)}.1 \\
&= x^{[(-i)j(-1)+(i)(-1)(j+l)]+[(-k)(-1)(j+l)+k(-1)(2j+l)]} \\
&= x^{i\{(-1)j(-1)+(-1)(j+l)\}+k\{(-1)(-1)(j+l)+(-1)(2j+l)\}}
\end{aligned}$$

Now consider a number of cases

(*i*) *j and l even :*

$$[\ ,\ ] = x^{i\{-1+1\}+k\{(-1)+1\}} = x^0 = 1$$

(*ii*) *j even and l odd :*

$$[\ ,\ ] = x^{i\{-1+(-1)\}+k\{1+(-1)\}} = x^{-2i}$$

(*iii*) *j odd and l even :*

$$[\ ,\ ] = x^{i\{1+(-1)\}+k\{1+1\}} = x^{2k}$$

(*iii*) *j and l odd :*

$$[\ ,\ ] = x^{i\{1+1\}+k\{-1+(-1)\}} = x^{2i-2k}$$

$$\therefore {D_{12}}' = \{1, x^2, x^4\} \cong C_3$$

$$\therefore D_{12}/{D_{12}}' \cong C_4 \text{ or } C_2 \times C_2 \text{ (considering sizes)}$$

Note : $D_{12} \cong D_6 \times C_2$ *also* $C_{12} \ncong C_6 \times C_2$ *but* $C_{12} \cong C_3 \times C_4$. $D_{12} \cong D_6 \times C_2 =< x^2, y \,|\, (x^2)^3 = y^2 = 1,\, y(x^2)y = (x^2)^{-1} > \times < x^3 > = \{x^{2i}.y^j.x^{3k} \,|\, i \in \{0,1,2\},\ j \in \{0,1\},\ k \in \{0,1\}\}$.

$$\therefore \frac{D_{12}}{{D_{12}}'} \cong \frac{D_6 \times C_2}{C_3} \cong \frac{D_6}{C_3} \times C_2 = C_2 \times C_2$$

$$\mathbb{F}_5 D_{12} \cong \mathbb{F}_5(C_2 \times C_2) \oplus NCP$$
$$\mathbb{F}_5 D_{12} \cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus NCP$$

$\therefore$ NCP has dimension 8. So $NCP \cong M_2(\mathbb{F}_5) \oplus M_2(\mathbb{F}_5)$ or $NCP \cong M_2(\mathbb{F}_{5^2})$.

So $\mathcal{U}(\mathbb{F}_5 D_{12}) \cong C_4 \times C_4 \times C_4 \times C_4 \times GL_2(\mathbb{F}_5) \times GL_2(\mathbb{F}_5)$ or $\mathcal{U}(\mathbb{F}_5 D_{12}) \cong C_4 \times C_4 \times C_4 \times C_4 \times GL_2(\mathbb{F}_{5^2})$.

$$|\mathcal{U}(\mathbb{F}_5 D_{12})| = (p-1)^4\{(p^2-1)(p^2-p)\}^2 = 4^4\{(24)(20)\}^2 = 2^{18}3^25^2$$

or

$$|\mathcal{U}(\mathbb{F}_5 D_{12})| = (p-1)^4\{(q^2-1)(q^2-q)\} = 4^4\{((5^2)^2-1)((5^2)^2-5^2)\}$$

Note that $D_{12} < \mathcal{U}(\mathbb{F}_5 D_{12}$ so $12 \mid |\mathcal{U}(\mathbb{F}_5 D_{12})|$. But 12 divides the order of both cases so this does not help to differentiate between them. Also, $U = \mathcal{U}(\mathbb{F}_5 D_{12}) \cong \mathcal{U}(\mathbb{F}_5(D_6 \times C_2)) > \mathcal{U}(\mathbb{F}_5 D_6)$ and $U > \mathcal{U}(\mathbb{F}_5 C_2)$.

Lemma 4.35 *$Z(M_n(K)) = I_{n\times n}.K$. Thus $dim_K(Z(M_n(K))) = 1$.*

Definition 4.36 *Let G be a finite group and R a commutative ring. Let $\{C_i\}_{i\in I}$ be the set of conjugacy classes of G. Then*

$$\widehat{C_i} = \sum_{c\in C_i} c \in RG$$

is called the ***class sum*** *of C_i.*

Theorem 4.37 *Let G be a group and R a commutative ring. Then the set of class sums $\{\widehat{C_i}\}$ of G forms a basis for $Z(RG)$ over R. Thus $Z(RG)$ has dimension t over R, where t is the number of conjugacy classes of G.*

Proof. Let $\widehat{C_i}$ be a class sum. Let $g \in G$. Then $\widehat{C_i}^g = \widehat{C_i}$. $\therefore \widehat{C_i} \in Z(RG)$. Let $\alpha = \sum a_g g \in Z(RG)$. Let $h \in G$. Then $\alpha^h = \alpha$ so $a_{g^h} = a_g$ (coefficient of g = coefficient of g^h). Thus the entire conjugacy class C_i has the same coefficient in the expansion of α. $\therefore \alpha = \sum_{i\in I} c_i\widehat{C_i}$ $(c_i \in R)$. $\therefore Z(RG) \subset$ {linear combinations of $\widehat{C_i}$ over R}.

$\therefore Z(RG) = \{\text{linear combinations of } \widehat{C}_i \text{ over } R\}$.

It remains to show linear independance of $\{\widehat{C}_i\}$. Suppose $\sum_{i \in I} c_i \widehat{C}_i = 0$. Then we have an R-linear combination of elements of G, but the elements of G are linear independant over R. So the coefficients are all 0.

$$\sum_{i \in I} c_i \widehat{C}_i = 0 \Longrightarrow c_i = 0 \; \forall \; i \in I$$

$\therefore \{\widehat{C}_i\}$ is linear independant over R. ■

Recall the class equation of a finite group G. Let $\{x_1, x_2, \ldots, x_t\}$ be a complete set of conjugacy class representatives of G. Let $c(x_i)$ = conjugacy class containing x_i. Let $n_i = |C(x_i)| = [G : C_G(x_i)]$. Then $|G| = \sum_{i=1}^{t} n_i$ $= \sum_{i=1}^{t} |C(x_i)| = \sum_{i=1}^{t} [G : C_G(x_i)] = |Z(G)| + \sum_{n_i > 1} n_i$. (Note : $n_i = 1 \Longleftrightarrow x_i \in Z(G)$).

Lemma 4.38 *Let G be a finite group and $\mathbb{C}$ the complex numbers. Then*

$$\mathbb{C}G \cong \oplus_{i=1}^{t} M_{n_i}(\mathbb{C})$$

where $t =$ the number of conjugacy classes of G.

Proof. $\dim_{\mathbb{C}} \mathbb{C}G = \sharp$ of conjugacy classes of G. $\therefore \dim_{\mathbb{C}} Z(\oplus_{i=1}^{t} M_{n_i}(\mathbb{C}))$ $= \sum_{i=1}^{t} \dim_{\mathbb{C}} Z(M_{n_i}(\mathbb{C})) = \sum_{i=1}^{t} 1 = t$. ■

Example 4.39 $\mathbb{F}_5 C_2 \cong \mathbb{F}_5 \oplus \mathbb{F}_5$. *Here $Z(\mathbb{F}_5 C_2) = \mathbb{F}_5 C_2$ so $dim_{\mathbb{F}_5} Z(\mathbb{F}_5 C_2) = dim_{\mathbb{F}_5}(\mathbb{F}_5 C_2) = 2 = \sharp$ of conjugacy classes of C_2. ($C_2 = \{1, x\} \Longrightarrow \{1\}$ and $\{x\}$ are the only conjugacy classes of C_2).*

Example 4.40 $\mathbb{F}_5 S_3 \cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus M_2(\mathbb{F}_5)$. *$S_3 =< x, y \,|\, x^n = y^2 = 1,\, yxy = x^{-1} >$. $S_3{}' =< x^2 >\cong C_3$. $\therefore S_3 \; S_3{}' \cong C_2$*

$$\begin{aligned} \therefore \mathbb{F}_5 S_3 &\cong \mathbb{F}_5 C_2 \oplus NCP \\ &\cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus NCP \\ &\cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus M_2(\mathbb{F}_5). \end{aligned}$$

$$\begin{aligned} \therefore Z(\mathbb{F}_5 S_3) &\cong Z(\mathbb{F}_5 \oplus \mathbb{F}_5 \oplus M_2(\mathbb{F}_5)) \\ &\cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus Z(M_2(\mathbb{F}_5)) \\ &\cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus I_{2\times 2}.\mathbb{F}_5 \\ &\cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5. \end{aligned}$$

This is a 3*-dimensional vector space over* $\mathbb{F}_5$ *(with basis* $\{(1,0,0),\ (0,1,0),\ (0,0,1)\}$*).* $\therefore S_3$ *has* 3 *conjugacy classes. We proved this group theory result using group rings.*

Now using group theory, find the 3 conjugacy classes of S_3.

Theorem 4.41 *Let* R *be a commutative ring and let* G *and* H *be groups. Then*

$$R(G \times H) \cong (RG)H.$$

Proof. Homework 2. ∎

Corollary 4.42

$$R(G \times H) \cong (RG)H \cong (RH)G$$

Proof. $R(G \times H) \cong R(H \times G)$ and now use the theorem. Note $G \times H \cong H \times G$ by $(g, h) \mapsto (h, g)$. ∎

Corollary 4.43

$$R(G_1 \times G_2 \times \cdots \times G_n) \cong (((RG_1)G_2)\ldots)G_n$$

Theorem 4.44 *Let $\{R_i\}_{i\in I}$ be a set of rings and let $R = \oplus_{i\in I} R_i$. Let G be a group. Then*

$$RG \cong (\oplus_{i\in I} R_i)G \cong \oplus_{i\in I}(R_i G).$$

Proof. Homework 2. ■

Example 4.45 $\mathbb{F}_5 C_6$. $\mathbb{F}_5 C_6 \cong \mathbb{F}_5(C_2 \times C_3) \cong (\mathbb{F}_5 C_2)C_3 \cong (\mathbb{F}_5 \oplus \mathbb{F}_5)C_3 \cong \mathbb{F}_5 C_3 \oplus \mathbb{F}_5 C_3$.

Now $\mathbb{F}_5 C_3 \cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5$ *or* $\mathbb{F}_5 C_3 \cong \mathbb{F}_5 \oplus \mathbb{F}_{5^2}$. $\therefore \mathcal{U}(\mathbb{F}_5 C_3) \cong C_4 \times C_4 \times C_4$ *or* $C_4 \times C_{24}$. *But* $C_3 < \mathcal{U}(\mathbb{F}_5 C_3)$, *so by lagrange's theorem ,* $3 \mid \mathcal{U}(\mathbb{F}_5 C_3)$. *However* $3 \nmid |C_4 \times C_4 \times C_4|$ *and* $3 \mid |C_4 \times C_{24}|$ *so* $\mathcal{U}(\mathbb{F}_5 C_3) \cong C_4 \times C_{24}$ *and* $\mathbb{F}_5 C_3 \cong \mathbb{F}_5 \oplus \mathbb{F}_{5^2}$.

$$\begin{aligned} \therefore \mathbb{F}_5 C_6 &\cong \mathcal{U}(\mathbb{F}_5 C_3) \oplus \mathcal{U}(\mathbb{F}_5 C_3) \\ &\cong \mathbb{F}_5 \oplus \mathbb{F}_{5^2} \oplus \mathbb{F}_5 \oplus \mathbb{F}_{5^2} \\ &\cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_{5^2} \oplus \mathbb{F}_{5^2} \end{aligned}$$

Theorem 4.46 (***Fundamental Theorem of Finite Abelian Groups***) *Let A be a finite abelian group. Then*

$$A \cong G_1 \times G_2 \times \cdots \times G_n$$

, where G_i is a cyclic group of order ${p_i}^{m_i}$, where p_i is some prime.

Example 4.47 *Let A be an abelian group of order* $30 = 2^1.3^1.5^1$. *Then*

$$\begin{aligned} A &\cong C_{30} \\ &\cong C_5 \times C_6 \\ &\cong C_5 \times C_3 \times C_2 \\ &\cong C_{15} \times C_2 \\ &\cong C_{10} \times C_3 \end{aligned}$$

These are all the same because 2,3 *and* 5 *are all relatively prime.*

$$\therefore A \cong C_2 \times C_3 \times C_5.$$

Example 4.48 $C_{24} \cong C_{2^3.3} \cong C_{2^3} \times C_3 \not\cong C_6 \times C_4 \cong C_2 \times C_3 \times C_4 \cong C_2 \times C_{2^2} \times C_3$.

Example 4.49

$$\begin{aligned} \mathbb{F}_7 C_{30} &\cong \mathbb{F}_7(C_2 \times C_3 \times C_5) \\ &\cong (\mathbb{F}_7 C_2)(C_3 \times C_5) \\ &\cong (\mathbb{F}_7 \oplus \mathbb{F}_7)(C_3 \times C_5) \\ &\cong (\mathbb{F}_7 \oplus \mathbb{F}_7)C_3)C_5) \\ &\cong (\mathbb{F}_7 C_3 \oplus \mathbb{F}_7 C_3)C_5) \\ &\cong (\mathbb{F}_7 C_3)C_5 \oplus (\mathbb{F}_7 C_3)C_5 \\ &\cong \ ? \end{aligned}$$

It is not obvious what $\mathbb{F}_7 C_3$ is ! (Lagrange's theorem doesn't help).

Hey Leo i thought I'd help you out here !!!

$\mathbb{F}_7 C_3 \cong \mathbb{F}_7 \oplus \mathbb{F}_7 \oplus \mathbb{F}_7$ (since $|\mathcal{U}(\mathbb{F}_7 C_3)| = 216 = 6^3$ and $\mathcal{U}(\mathbb{F}_7 C_3) \cong C_6 \times C_6 \times C_6$). So $\mathbb{F}_7 C_{30} \cong (\mathbb{F}_7 \oplus \mathbb{F}_7 \oplus \mathbb{F}_7)C_5 \oplus (\mathbb{F}_7 \oplus \mathbb{F}_7 \oplus \mathbb{F}_7)C_5 \cong \{\oplus_{i=1}^3 \mathbb{F}_7\}C_5 \oplus \{\oplus_{i=1}^3 \mathbb{F}_7\}C_5 \cong \{\oplus_{i=1}^6 \mathbb{F}_7\}C_5 \cong \oplus_{i=1}^6 \{\mathbb{F}_7 C_5\}$. Also $\mathbb{F}_7 C_5 \cong \mathbb{F}_7 \oplus \mathbb{F}_{7^4}$ (since $|\mathcal{U}(\mathbb{F}_7 C_5)| = 14400 = (7-1)(7^4-1)$ and $\mathcal{U}(\mathbb{F}_7 C_5) \cong C_6 \times C_{2400}$) so $\mathbb{F}_7 C_{30} \cong \oplus_{i=1}^6 \{\mathbb{F}_7 \oplus \mathbb{F}_{7^4}\}$.

$$\therefore \mathbb{F}_7 C_{30} \cong \oplus_{i=1}^6 \mathbb{F}_7 \oplus_{i=1}^6 \mathbb{F}_{7^4}$$

Example 4.50 $\mathbb{F}_5 D_{12} \cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus M_2(\mathbb{F}_5) \oplus M_2(\mathbb{F}_5)$ *or* $\mathbb{F}_5 D_{12} \cong \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus M_2(\mathbb{F}_{5^2})$.

We mentioned before that $D_{12} \cong D_6 \times C_2$. $\therefore \mathbb{F}_5 D_{12} \cong \mathbb{F}_5(C_2 \times D_6) \cong (\mathbb{F}_5 C_2)D_6 \cong (\mathbb{F}_5 \oplus \mathbb{F}_5)D_6 \cong \mathbb{F}_5 D_6 \oplus \mathbb{F}_5 D_6$.

$\therefore \mathbb{F}_5 D_{12} \cong (\mathbb{F}_5 \oplus \mathbb{F}_5 \oplus M_2(\mathbb{F}_5)) \oplus (\mathbb{F}_5 \oplus \mathbb{F}_5 \oplus M_2(\mathbb{F}_5)) \cong \oplus_{i=1}^4 \mathbb{F}_5 \oplus \oplus_{j=1}^2 M_2(\mathbb{F}_5)$.

Note : $\mathbb{C}S_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$ but $\mathbb{Q}S_3 \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{H}$ where $\mathbb{H}$ is the division ring of quaternions over $\mathbb{Q}$.

The End

Appendix A

Extra's

A.1 Homework 1 + Solutions

Homework 1

Q1 For the following group rings, **(i)** find the group of units and show what abstract group it is isomorphic to, **(ii)** find the augmentation ideal and **(iii)** fing the set of zero-divisors.

(a) $\mathbb{Z}_2 C_2$.

(b) $\mathbb{Z}_{11} C_1$.

(c) $\mathbb{Z}_2 C_3$.

(d) $\mathbb{Z}_3 C_3$.

(e) $\mathbb{Z}_2 C_4$.

(f) $\mathbb{Z}_2 C_2 \times C_2$.

(g) $\mathbb{Z}_2 S_3$.

What conjectures can you come up with after doing these examples ?

(g) $\mathcal{U}(\mathbb{Z}_2 S_3)$ contains 12 elements. Find these 12 elements and find the abstract group of order 12 which $\mathcal{U}(\mathbb{Z}_2 S_3)$ is isomorphic to. (Hint : use $x + \widehat{S_3} + y + \widehat{S_3}$ where $\widehat{S_3} = 1 + x + x^2 + y + xy + x^2 y$). (ignore the zero-divisors for (g)).

Note : Bonus question (optional).

(h) Find the zero-divisors of $\mathbb{Z}_2 S_3$.

Solutions

A.2 Homework 2 + Solutions

Homework 2

Q1 Find the abstract group structure of $\mathcal{U}(\mathbb{F}_2 D_{12})$. Hints :

1 Note that Maschke's theorem does not apply.

2 $D_{12} \cong C_2 \times D_6$.

3 $\mathcal{U}(\mathbb{F}_2 D_6) \cong D_{12}$

Q2 Find the size of the group $\mathcal{U}(\mathbb{F}_2 D_{12})$. Hint : $|\mathcal{U}(\mathbb{F}_3 D_6)| = 324$.

Q3 (a) Show that $D_8^{'} \cong C_2$.

(b) Show that $D_8/D_8^{'} \cong C_2 \times C_2$.

(c) Conclude that $\mathbb{F}_p D_8 \cong (\oplus_{i=1}^4 \mathbb{F}_p) \oplus M_2(\mathbb{F}_p)$. (where $p \neq 2$).

Q4 (a) Find all the conjugacy classes of D_8 (there are 5).

(b) What is $\dim_{\mathbb{F}_p} Z(\mathbb{F}_p D_8)$.

(c) Conclude that $\mathbb{F}_p D_8 \cong (\oplus_{i=1}^4 \mathbb{F}_p) \oplus M_2(\mathbb{F}_p)$. (where $p \neq 2$).

Q5 Let R be a commutative ring and let G and H be groups. Prove that

$$R(G \times H) \cong (RG)H.$$

Q6 Let $\{R_i\}_{i\in I}$ be a set of rings and let G be a group. Let $R = \oplus_{i\in I}$. Show that $RG \cong \oplus_{i\in I} R_i G$.

Q7 The quaternion group of 8 elements has the following presentation:

$$\mathbb{H} =< a, b \,|\, a^4 = 1,\ a^2 = b^2,\ bab^{-1} = a^{-1} >$$

(a) Show that $\mathbb{H}^{'} =< a^2 >$

(b) Show that $\mathbb{H}/\mathbb{H}^{'} \cong C_2 \times C_2$.

(c) Conclude that $\mathbb{F}_p D_8 \cong (\oplus_{i=1}^4 \mathbb{F}_p) \oplus M_2(\mathbb{F}_p)$. (where $p \neq 2$).

Q8 We showed in class that either

$$\mathbb{F}_3 D_{10} \cong \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus M_2(\mathbb{F}_3) \oplus M_2(\mathbb{F}_3)$$

or

$$\mathbb{F}_3 D_{10} \cong \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus M_2(\mathbb{F}_{3^2})$$

Use lagranges theorem to determine which one of the two isomorphisms above applies.

Q9 Using the presentation of $\mathbb{H}$ given in Q7, show that $< \widehat{a} >$ is a central idempotent of $\mathbb{F}_3\mathbb{H}$. List all the elements of $ann_r\Delta(\mathbb{H}, < a >)$ in the group ring $\mathbb{F}_3\mathbb{H}$.

Q10 Find $|GL_3(\mathbb{F}_{p^n})|$.

Solutions

A.3 Autumn Exam + Solutions