IMMERSE Algebra Course
Notes from Donald Passman's
Prime and Semi-prime Group Rings

12 - 13 July, 2005

First Lecture - An Introduction

1 Introduction and Review of Rings

Let R be a ring with operations $+$ and $\cdot$. We will assume that R has unity, but is not necessarily commutative. Let $I \triangleleft R$ be an ideal, that is I is closed under addition and $IR \subset I$ and $RI \subset I$.

Let $\phi : R \to S$ be a homorphism. Then $\ker(\phi) = \{r \mid \phi(r) = 0\} \triangleleft R$. Conversely if $I \triangleleft R$ there is a quotient ring R/I and a homomorphism $\psi : R \to R/I$ with $\ker\psi = I$. Therefore there is a one-to-one correspondence between ideals of a ring and kernels of homomorphisms.

Let $\phi : R \twoheadrightarrow S$. Then if $\ker\phi = I$, there is an isomorphism theorem showing $S \cong R/I$.

Every ring R has two silly ideals, called trivial ideals:

1. $I = \{0\}$
2. $I = R$

Definition 1 *R is simple iff the only ideals are trivial.*

Example 1 *Let F be a field or a division ring. Then $M_n(F)$, the $n \times n-$matrices over F form a ring. This is a simple ring, meaning there are no intermediate ideals.*

Definition 2 *If $I, J \triangleleft R$ then new ideals can be formed in the following ways:*

1. *$I + J = \{i + j \mid i \in I, j \in J\} \lhd R$*

2. *$I \cap J \lhd J$*

   These first two are commutative operations on ideals.

3. *$IJ \lhd J$ where $IJ =$ the ideal generated by $\{xy \mid x \in I, y \in J\}$, so really it consists of finite sums of these products. This operation on ideals is not commutative.*

Example 2 *Let R be the ring of upper triangular $2 \times 2-$ matrices over a field, F, so*

$$R = \left\{ \left(\begin{array}{cc} * & * \\ 0 & * \end{array} \right) \middle| * \in F \right\}$$

Let $\phi : R \to F$ be given by $\left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \mapsto a$. Then $\ker \phi = I = \left\{ \left(\begin{array}{cc} 0 & * \\ 0 & * \end{array} \right) \middle| * \in F \right\}$.

Let $\psi : R \to F$ be given by $\left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \mapsto c$. Then $\ker \psi = I = \left\{ \left(\begin{array}{cc} * & * \\ 0 & 0 \end{array} \right) \middle| * \in F \right\}$.

Then $IJ = 0$ but $JI = \left(\begin{array}{cc} 0 & * \\ 0 & 0 \end{array} \right)$, so these operations are not commutative.

Definition 3 *A ring R is prime if whenever $I, J \lhd R$ and $IJ = 0$, then $I = 0$ or $J = 0$.*

Note. Any simple ring is prime. However the converse is not necessarily true, for example think of ideals of $\mathbb{Z}$.

In particular, $M_n(F)$, as defined above, is a prime ring, but has zero divisors. In other words, there exist elements, $a, b \neq 0$ where $ab = 0$. A ring without zero divisors is called a domain.

Note. A domain is a prime ring, but the converse does not necessarily hold.

Definition 4 *A ring R is semiprime iff if $I \lhd R$ and $I^2 = 0$ then $I = 0$, i.e. there are no nontrivial ideals of square zero.*

Definition 5 *If $P \lhd R$ then P is prime iff R/P is a prime ring. Equivalently, P is prime iff if $I, J \lhd R$ and $IJ \subset P$ then $I \subset P$ or $J \subset P$.*

Lemma 1 *R is semiprime iff $\displaystyle\bigcap_{P \text{ prime ideal}} P = 0$*

Definition 6 *Let R be a ring. Then the center of the ring is $Z(R) = \{r \in R \mid rx = xr \ \forall \ x \in R\}$.*

Notice that $Z(R)$ is a commutative subring of R. In particular, if $a \in R$ then $aR \triangleleft R$ so it is an ideal. In general, one would need to check that $RaR \triangleleft R$, but commutativity reduces this to the statement above.

If $a, b \in Z(R)$ and $ab = 0$ then $aR \cdot bR = 0$ since $aR = Ra$. Therefore if $Z(R)$ has zero divisors the ring cannot be prime.

Lemma 2 *If R is prime then $Z(R)$ is a domain. If R is semiprime then $Z(R)$ is a reduced ring (that is there are no elements of square zero).*

Example 3 *If $R = \left\{ \left(\begin{array}{cc} * & * \\ 0 & * \end{array} \right) \middle| * \in F \right\}$, then $I \cap J = N = \left\{ \left(\begin{array}{cc} 0 & * \\ 0 & 0 \end{array} \right) \middle| * \in F \right\} \triangleleft R$ and $N^2 = 0$. So this ring isn't semiprime, and therefore it is not prime.*

Assumer $\left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \in Z(R)$. Then for it to commute with $\left(\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array} \right)$ we need $b = 0$, and for it to commute with $\left(\begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array} \right)$ we need $a = c$. Therefore the center is

$$Z(R) = \left\{ \left(\begin{array}{cc} a & 0 \\ 0 & a \end{array} \right) \mid a \in F \right\}$$

which are the scalar matrices. Therefore in this case, $Z(R) \cong F$. Therefore $Z(R)$ is a field, so it is not a domain.

2 Group Rings

To define group rings, let K be a field and G a multiplicative group. Then $K[G]$ is a group algebra. We allow infinite groups, but will restrict ourselves to elements with finite support. Therefore, $K[G]$ is a vector space over K with G as a basis, so elements are finite sums of the form $\sum_{g \in G} k_g g$.

Example 4 *$K[x]$ has $K-$basis $\{1, x, x^2, \ldots\} = S$. Notice that S is a semigroup because there are no inverses. If $G = \langle x \rangle$, the infinite cyclic group, then $G = \{\ldots, x^{-2}, x^{-1}, 1, x, x^2, \ldots\}$ and the elements of $K[G] = K[x, x^{-1}] = \sum k_i x^i$, the Laurent polynomials.*

Let $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle$, the product of finitely many infinite cyclic groups. Then $K[G] = K[x_1, x_1^{-1}, x_2, , x_2^{-1} \ldots, x_n, x_n^{-1}]$. This is a commutative domain (i.e. no zero divisors).

If $\phi : G \to H$ is a homomorphism, then there exists a homomorphism $\overline{\phi} : K[G] \to K[H]$, where you extend the map on the basis to the group algebra.

If $H \subset G$ then $K[H] \subset K[G]$.

Lemma 3 *Suppose G is abelian and torsion free (i.e. there are no elements of finite order) then $K[G]$ is a commutative domain.*

Proof. Suppose $\alpha, \beta \in K[G]$. If $\alpha\beta = 0$ then let $H \subset G$ be generated by the support elements of α and β. Then $\alpha, \beta \in K[H]$. Now H is a finitely generated torsion free abelian group, so $H = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle$, so from earlier, there are no zero divisors in H. Therefore is $\alpha, \beta \in K[H]$ and $\alpha\beta = 0$ then either $\alpha = 0$ or $\beta = 0$.

□

Let G be finite, and define the norm element, $\widehat{G} = \sum_{g \in G} g \in K[G]$. Notice that $gG = G$ since this just shuffles the elements in G. Therefore, $g\widehat{G} = \widehat{G}$. In particular $\widehat{G}\widehat{G} = \mid G \mid \widehat{G}$. Therefore, $\widehat{G}\left(\widehat{G} - \mid G \mid\right) = 0$ so there exist zero divisors, and they are nontrivial if $\mid G \mid > 1$ since this is the only time that $\widehat{G} - \mid G \mid = 0$.

3 Main Results

Theorem 4 *(P. Jordan) If $char(K) = 0$ then $K[G]$ is semiprime.*

If $\psi : G \to \overline{G}$ is a homomorphism then $\ker \psi = \{g \mid \psi(g) = 1\}$ is a normal subgroup. In fact, $N \triangleleft G$ iff $N \subset G$ and if either

1. $gN = Ng \; \forall \; g \in G$
2. $gNg^{-1} = N \; \forall \; g \in G$ or $g^{-1}Ng = N$, i.e. normal subgroups are stable under conjugation.

As before, normal subgroups are in one-to-one correspondence with the kernels of homomorphisms.

Theorem 5 *(Passman) If $char(K) = p$ then TFAE:*

1. *$K[G]$ is semiprime*
2. *$Z(K[G])$ is reduced, so there are no elements of square zero*
3. *G has no finite normal subgroups with order divisible by p*

Theorem 6 *(Connell) TFAE*

1. *G has no finite normal subgroups except $\langle e \rangle$.*

2. *$Z(K[G])$ is domain.*

3. *$K[G]$ is prime.*

Proof.

(1) $\Rightarrow$ (2) : Suppose N is a finite normal subgroup. Then $K[N] \subset K[G]$, and $\widehat{N} = \sum_{n \in N} n$. Then $\widehat{N}\left(\widehat{N} - \mid N \mid\right) = 0$. Since $N \triangleleft G$, $gN = Ng$ and so $g\widehat{N} = \widehat{N}g$, so $\widehat{N} \in Z(K[G])$. Therefore this is not a domain.

If $char(K) = p$ and p divides $\mid N \mid$, then $\mid \widehat{N} \mid \cong 0(\mod p)$ and threfore $Z(K[G])$ has no zero divisors.

(2) $\Rightarrow$ (3) : If $Z(K[G])$ has zero divisors then $K[G]$ is not prime in general. Similarly for Passman.

(3) $\Rightarrow$ (1) will be proved later.

□

Proof of Jordan. Let $char(K) = 0$. Let $o \neq I \triangleleft K[G]$ and $I^2 = 0$. Take $0 \neq \alpha \in I$. Then there exists a finitely generated field $F \subset K$ so that $\alpha \in F[G]$. Now $I \cap F[G]$ is a non-zero ideal with square 0. So we can assume $K = F$ is finitely generated.

Since K is finitely generated, we can know $K \subset \mathbb{C}$, so $K[G] \subset \mathbb{C}[G]$. Therefore, $\mathbb{C} \cdot I$ gives an ideal in $\mathbb{C}[G]$ and by commutativity $(\mathbb{C} \cdot I)^2 = 0$. Therefore, examine $\mathbb{C}[G]$ and define an involution, $*$, in the following way:

$$* : \mathbb{C}[G] \to \mathbb{C}[G]$$

with

$$\sum k_g g \mapsto \sum \overline{k_g} g^{-1}.$$

To proceed, we need the following lemma:

Lemma 7

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

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

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

$$\alpha \cdot \alpha^* = 0 \iff \alpha = 0$$

Proof of Lemma.

$$\begin{aligned} \alpha \cdot \alpha^* &= \sum k_g g \cdot \sum \overline{k_g} g^{-1} \\ &= \cdots + k_g \overline{k_g} g g^{-1} + \cdots \\ &= \sum \mid k_g \mid^2 \cdot 1 \end{aligned}$$

Therefore $\sum \mid k_g \mid^2 = 0 \iff \mid k_g \mid = 0 \; \forall \; k_g \in \mathbb{C}$. $\square$

Therefore, $0 \neq I \triangleleft \mathbb{C}[G]$ and $0 \neq \alpha \in I$. Then

$$\beta = \alpha\alpha^* \in I \Rightarrow \beta \neq 0$$

$$\beta^* = \alpha^{**}\alpha^* = \alpha\alpha^* = \beta$$

$I^2 = 0$ so $0 = \beta\beta = \beta\beta^*$ which is a contradiction since $\beta \neq 0$.

$\square$

Second Lecture - Proofs of the Main Results

It remains to prove:

1. (Prime case) If $I, J \triangleleft K[G]$ and $I, J \neq 0$ and $IJ = 0$ then there exists a finite normal subgroup $N \neq 1$.
2. (Semiprime case) If $0 \neq I$, $I^2 = 0$ then there exists a finite $N \triangleleft G$ where $p| \mid N \mid$.

Suppose that $H < G$. Then $K[H] < K[G]$ and there exists a map

$$\pi_H : K[G] \to K[H]$$

given by

$$\sum_{g \in G} k_g g \mapsto \sum_{g \in H} k_g g$$

Notice that this is the forgetful map - elements that are not in H are forgotten about, and become 0. This is not a multiplicative map, unless $H = G$ in which case this is the identity map.

However, if $G \neq H$ and $g \in G \setminus H$ then $\pi_H(g) = 0$ and $\pi_H(g^{-1}) = 0$, but $\pi_H(gg^{-1}) = \pi_H(1) = 1$.

Lemma 8 *π_H is a $K[H]$ bimodule map, i.e.*

1. $\pi_H(\alpha + \beta) = \pi_H(\alpha) + \pi_H(\beta)$
2. *If $\gamma \in K[H]$ then $\pi_H(\alpha\gamma) = \pi_H(\alpha) \cdot \gamma$ and $\pi_H(\gamma\alpha) = \gamma \cdot \pi_H(\alpha)$.*

This is because if we let $g, h \in H$, there are two possibilities:

1. If $g \in H$ then $gh \in H$
2. If $g \notin H$ then $gh \notin H$

Lemma 9 *Let $H < G$.*

1. *If $I \triangleleft K[G]$ then $\pi_H(I) \triangleleft K[H]$*
2. *If $I \neq 0$ then $\pi_H(I) \neq 0$*

Proof.

1. Let $\pi_H(\alpha), \pi_H(\beta) \in \pi_H(I)$. Then $\pi_H(\alpha) + \pi_H(\beta) = \pi_H(\alpha + \beta) \in \pi_H(I)$ since $\alpha + \beta \in I$.

   Let $\gamma \in K[H]$. Then $\pi_H(\alpha)\gamma = \pi_H(\alpha\gamma)$. But if $\alpha \in I$ then $\alpha\gamma \in I$. So $\pi_H(\alpha\gamma) \in \pi_H(I)$. Similarly on the left. Therefore, $\pi_H(I) \triangleleft K[H]$.

2. Let $\alpha \in I$, $\alpha \neq 0$. Then $\alpha = \sum k_g g$. Assume $k_x \neq 0$. Then

$$\alpha x^{-1} \in I$$

$$\alpha x^{-1} \in \sum k_g g x^{-1}$$

   Notice that when $g = x$, $gx^{-1} = 1$. Therefore

$$\alpha x^{-1} = k_x 1 + \cdots$$

   Since $1 \in H$, $k_x 1 \in K[H]$ so $\pi_H(I) \neq 0$

□

Let $N \triangleleft G$ and N be finite. Pick $g \in N$. Then $\circ(g) < \infty$. Multiplying by G permutes the elements of G by conjugation, so

$$g \mapsto g^x = x^{-1} g x$$

is an automorphism of the group. Notice that $N^x = x^{-1} N x = N$ since $N \triangleleft G$. Therefore, if $g \in N$, then there are only finitely many conjugates of g.

The number of conjugates of an arbitrary element $g \in G$ is $[G : C_G(g)]$, the index of $C_G(g)$ in the group G. Notice that $C_G(x)$ is the centralizer of the element g in G, namely

$$C_G(g) = \{x \in G \mid xg = gx\}$$

the set of elements in G that commute with g. Notice that if $C_G(g) = G$ then the only conjugate of g is itself. The conjugates of g are in one-to-one correspondence with the cosets of the centralizer. So in finite normal subgroups, elements have finite order and finitely many conjugates.

Lemma 10 *(Schur) If G is a group and $[G : Z(G)] < \infty$, i.e. it is center-by-finite, then $\mid G' \mid < \infty$, where G' is the commutator subgroup.*

Lemma 11 *If g has finite order and a finite number of conjugates then $g \in N$ for some finite normal subgroup N.*

Proof. Let $g_1, g_2, \ldots, g_n$ be conjugates of g. Let $N = \langle g_1, g_2, \ldots, g_n \rangle$. Notice that conjugation by g permutes the generators, so $N \triangleleft G$ and $g \in N$. It remains to prove N is finite. Therefore,

$$[N : C_N(g_i)] < \infty \ \forall \ g_i \in N$$

It remains to prove if you have a bunch of subgroups with finite index, then the intersection has finite order, so

$$\left| N : \bigcap C_n(g_i) \right| < \infty$$

Notice that $\bigcap C_n(g_i)$ contains all the elements that commute with all of the generators of N. So $\bigcap C_n(g_i) = Z(N)$ so it is center-by-finite so by Schur's lemma, N' is finite.

Look at N/N' which is an abelian group generated by the images of $g_1, g_2, \ldots, g_n$. Therefore it is abelian and finitely generated and all generator elements have finite order. Therefore N/N' is finite. Therefore N is finite. □

Definition 7 *Define $\Delta(G) = \{g \in G \mid \; [G : C_G(g)] < \infty\}$ is called the finite conjugate center, or FC center, i.e. there are a finite number of conjugates.*

Lemma 12 $\Delta(G) \subset G$. *Moreover it is normal (in fact it is characteristic). If $\Delta(G)$ has no elements of finite order other than e, then it is torsion free abelian.*

Proof. Let $g, h \in \Delta$. Each has only finitely many conjugates.

$$(gh)^x = g^x h^x$$

is an automorphism. Since there are finitely many conjugates for each g and h on the right, there are a finite number of conjugates on the left.

Therefore, this is a normal subgroup. If there are no elements of finite order, it is abelian. Assume Δ has no elements of finite order. Let $g, h \in \Delta$. We want to show that $gh = hg$. Look at $\langle g, h \rangle$. This is center-by-finite, so $\langle g, h \rangle$ is finite by Schur. But there are no elements of finite order, so $\langle g, h, \rangle' = 1$. Therefore $\langle g, h, \rangle$ is abelian □

Linear Identities

Let $\alpha_i, \beta_i \in K[G]$. Then if $\alpha_1 x \beta_1 + \alpha_2 x \beta_2 + \cdots + \alpha_n x \beta_n = 0$ for all $x \in G$. Linear identities in a group ring can be reduced to $\Delta-$subgroups.

Lemma 13 *(Δ-methods) Given $\sum \alpha_i x \beta i = 0 \; \forall \; x \in G$. Let $\pi_\Delta = \theta$. Then*

1. $\sum \theta(\alpha_i)\beta_i = 0$
2. $\sum \alpha_i \theta(\beta_i) = 0$
3. $\sum \theta(\alpha_i)\theta(\beta_i) = 0$

Proof. Need to show that (1) or (2) holds. Notice that (1) $\Rightarrow$ (3) since

$$0 = \sum \theta(\alpha_i)\beta_i$$

$$0 = \theta(0) = \sum \theta(\theta(\alpha_i)\beta_i)$$

Notice that $\theta(\alpha_i)\beta_i$ is in the subgroup.

$$0 = \sum \theta(\alpha_i)\theta(\beta_i)$$

since θ is a bimodule map. □

Corollary 14 *If $I, J \in K[G]$ and $IJ = 0$ then $\theta(I)\theta(J) = 0$ in $K[\Delta]$.*

Therefore if $K[G]$ is not prime, $K[\Delta]$ not prime, so it reduces to the FC-center.

Proof. Let $\alpha \in I$ and $\beta \in J$ then if $x \in G$, $x\beta \in J$.

$$\alpha x \beta = 0$$

since $IJ = 0$. Notice that $\alpha x \beta$ is a linear identity since it is true $\forall x \in G$. So $\theta(\alpha)\theta(\beta) = 0$. □

Proof of Connell's Theorem - Prime Case Assume that $0 \neq I, J \lhd K[G]$ with $IJ = 0$. We want to find a finite normal subgroup. Then $\theta(I)\theta(J) = 0$ where $0 \neq \theta(I)\theta)J) \lhd K[\Delta]$. Notice that they are non-zero because the map is a projection map. Therefore, $K[\Delta]$is not a domain, i.e. there exist zero divisors. Recall that if the group is torsion-free abelian then $K[G]$ is a domain, so Δ is not torsion-free abelian. Therefore, Δ contains elements of finite order, say $g \in \Delta, g \neq 1, \circ(g) < \infty$. Since$g \in$FC center, it has finitely many conjugates. So g is an element of a finite normal subgroup, N. □

Proof of Passman - Semiprime Case Let $char = p$, so that $pR = 0$. If R is commutative then the "Freshman's Dream" holds:

$$(a + b)^p = a^p + b^p$$

We need the following lemma:

Lemma 15 *(Brauer) In an arbitrary ring,*

$$(a_1 + a_2 + \cdots + a_n)^p = a_1^p + a_2^p + \cdots a_n^p + b$$

where $b \in [R, R]$, the Lie products.

In an arbitrary ring, $[a, b] = ab - ba$, and $[R, R]$ consists of finite sums of Lie products. Define the trace map

$$tr : K[G] \to K$$

given by

$$\sum k_g g \mapsto k_1$$

This is the same as the projection map $\pi_{\langle e\rangle}$. For a trace map we want $tr(\alpha\beta) = tr(\beta\alpha)$. So if $xy = 1$ then $yx = 1$. In particular, $tr([\alpha, \beta]) = 0$, so the trace kills Lie brackets.

Returning to the above line of reasoning:

Let $0 \neq I \triangleleft K[G]$ with $I^2 = 0$. Then

$$\theta(I) \neq 0$$

$$\theta(I) \triangleleft K[\Delta]$$

$$\theta(I)^2 = 0$$

So there exists $\alpha \in \theta(I)$ with $\alpha = \sum a_g g$ with $a_1 \neq 0$. So

$$\alpha^2 = 0 \Rightarrow \alpha^p = 0$$

$$\alpha^p = 0 = \sum a_g^p g^p + \beta$$

where β is the error by Brauer. Then

$$tr(0) = 0 = tr(\alpha^p)$$

So

$$o = \sum_{g^p=1} a_g^p$$

In particular, since $a_1 \neq 0 \Rightarrow \exists g \neq 1$ with $a_g \neq 0$. Therefore, since $g^p = 1$ there exists and element of order p in Δ. Therefore, there is an element of finite order. Which means that $g \in N$ where N is a finite normal subgroup with $\circ(g) \mid \mid N \mid$, i.e. $p \mid\mid N \mid$. $\square$