1 Spring 2002 – Ring Theory

Problem 1.1. Let R be a ring and A and B two non–isomorphic simple, left R–modules (a left–module is simple if it has no proper submodules, i.e., submodules other than $\{0\}$ and itself). Show that the only proper submodules of $M = A \oplus B$ are $\{(\alpha, 0) : \alpha \in A\}$ and $\{(0, \beta) : \beta \in B\}$.

Solution: This follows directly from the definitions and the projection maps. Suppose $N \subset M$ is a proper submodules. Define

$$\pi_A : N \longrightarrow A : (\alpha, \beta) \mapsto \alpha.$$

π_A is easily checked to be a homomorphism (since operations are componentwise). We claim that $\pi_A(N) \subset A$ is a submodule: suppose $a \in \pi_A(N)$, then $(\exists (a, \beta) \in N)(\pi_A((a, \beta) = a)$. Since N is a submodule, we have

$$-(a, \beta) = (-a, -\beta) \in N \Rightarrow \pi_A(-a, -\beta) = -a \Rightarrow -a \in \pi_A(N).$$

One can similarly show that $ra \in \pi_A(N), \forall r \in R$. Finally if $a, b \in \pi_A(N)$, then

$$[\exists (a, \beta), (a', \gamma) \in N][\pi_A((a, \beta) = a, \pi_A((a', \gamma) = a'],$$

so then $\pi_A((a, \beta) + (a', \gamma)) = \pi_A((a + b, \alpha + \gamma)) = a + b$, so $a + b \in \pi_A(N)$.

Similarly we can define π_B to project onto B and show that $\pi_B(N) \subset B$ is a submodule. By assumption it must be the case that $\pi_A(N) = \{0\}, A$ and $\pi_B(N) = \{0\}, B$ so that the only proper submodules of $\pi_A(N) \oplus \pi_B(N)$ are $\{(\alpha, 0) : \alpha \in A\}$ and $\{(0, \beta) : \beta \in B\}$. We are done since $N \subset \pi_A(N) \oplus \pi_B(N)$ (if $(a, b) \in N$, then $\pi_A((a, b)) = a \in \pi_A(N)$ and $\pi_B((a, b)) = b \in \pi_B(N)$, so $(a, b) \in \pi_A(N) \oplus \pi_B(N)$) so any submodule of N is also a submodule of $\pi_A(N) \oplus \pi_B(N)$. □

- Ring: A ring R is a set with two binary operations: $+$ and $\times$, such that
  - $(R, +)$ is an abelian group.
  - $\times$ is associative.
  - The distributive law holds.

  A ring is commutative if multiplication is commutative. A ring has an identity if $\exists 1 \in R$ such that $1 \times r = r \times 1 = r, \forall r \in R$. An example of a ring which is not a field is the integers $\mathbb{Z}$ under the usual operations.

- Module: Let R be a ring. A (left) R–module is a set M together with

- A binary operation $+$ such that $(M, +)$ is an abelian group.
- A map $R \times M \to M : (r, m) \mapsto rm$ such that
  - $(r + s)m = rm + sm$
  - $(rs)m = r(sm)$
  - $r(m + n) = rm + rn$
  - $1m = m, \forall m \in M$, if R has an identity.

$N \subset M$ is a submodule if it is a subgroup under addition and such that

$$(\forall r \in R, n \in N)(rn \in N).$$

If R is a field, then a module over R is also called a vector space. Abelian groups are all $\mathbb{Z}$–modules.

- Direct Sum (of modules): Let R be a ring. Let A, B be R–modules.
  - The (external) direct sum of A and B is the set

    $$A \times B = \{(a, b) \mid a \in A, b \in B\},$$

    with componenetwise addition and multiplication by elements of R.
  - Let A, B be submodules of an R module M. The following are equivalent:
    (1) $\pi : A \times B \longrightarrow A + B : (a, b) \mapsto a + b$ is an isomorphism.
    (2) $A \cap B = 0$.
    (3) Each $m \in A + B$ can be written uniquely as $a + b$, with $a \in A, b \in B$.
    If any of these three conditions are satisfied, then $M = A + B$ is the (internal) direct sum of A and B, written

    $$(A + B =)M = A \oplus B.$$

    Note that π is an isomorphism between $A \times B$ and $A \oplus B (= A + B)$.

- Projection: Let R be a ring. Let $M = A_1 \times A_2$ where A_1 and A_2 are R–modules. Then the maps

  $$\pi_i : M \longrightarrow A_i : (a_1, a_2) \mapsto a_i$$

  is a surjective homomorphism with

  $$\ker(\pi_i) = \{(a_1, a_2) \mid a_i = 1, a_j \in A_j\} \cong A_j \quad (j \neq i).$$

Problem 1.2. Let R be a commutative local ring, that is, R has a unique maximal ideal M.

(i) Show that if x lies in M, then $1-x$ is invertible.

(ii) Show that if R is Noetherian and I is an ideal satisfying $I^2 = I$, then $I = 0$. Hint: consider a minimal set of generators for I.

Solution: (i) Suppose $1-x$ is not invertible. Then consider $(1-x)$, the ideal generated by $1-x$. $(1-x)$ is contained in some maximal ideal, but since M is the unique maximal ideal, $(1-x) \subset M$. This implies that in particular $1-x \in M$, but then

$$1 = (1-x) + x \in M,$$

which is a contradiction since then $1 \cdot R \subset M \Rightarrow M = R$.

(ii) Since R is Noetherian, I is finitely generated (suppose it is not, then consider the chain

$$(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \dots,$$

where $x_i \in I$ and $x_i \notin (x_1, \dots, x_{i-1})$, if possible. $(x_1, x_2, \dots, x_n) \subset I$ for all n, so since I is not finitely generated, this chain does not stabilize (i.e. $\nexists k \in \mathbb{N}$ such that $(x_1, x_2, \dots, x_m) = (x_1, x_2, \dots, x_k)$ for all $m \geq k$), a contradiction). Let $\{x_1, x_2, \dots, x_n\}$ be a minimal set of generators for I. If $r \in I$, then

$$r = \sum_1^n a_i x_i, \quad a_i \in R$$

hence

$$r^2 = (\sum_1^n a_i x_i)^2 = x_1(a_1 \sum_1^n a_i x_i) + \dots + x_n(a_n \sum_1^n a_i x_i) = \sum_1^n r_i x_i,$$

where now $r_i \in I$. Since $I^2 = I$, there exists some $r \in I$ such that $r^2 = x_n$. So applying the above to x_n, we get that

$$x_n = \sum_1^n r_i x_i, \quad r_i \in I.$$

Therefore we have

$$(1 - r_i)x_n = r_1 x_1 + \dots + r_{n-1} x_{n-1}.$$

By (i), $(1 - r_i)$ is invertible, so multiplying both sides by its inverse we get

$$x_n = r_1' x_1 + \dots + r_{n-1}', \quad r_i' \in I,$$

which implies that $I = (x_1, x_2, \dots, x_{n-1})$, contradicting the minimality of n. $\square$

- Ideal: Let R be a ring. $I \in R$ is a (left) ideal of R if
  - I is a subring of R.
  - $rI \subset I, \forall r \in R$.

  A trivial consequence of the second item is that if an ideal contains 1, then it must be equal to the entire ring.

- Generators of Ideals: Let R be a ring with 1 and let $A \subset R$. Then the (left) ideal generated by A is the set

$$\{r_1a_1 + r_2a_2 + \dots r_na_n \mid r_i \in R, a_i \in A, n \in \mathbb{N}\},$$

  that is the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$.

- Local Ring: A commutative ring with 1 is a local ring if it has a unique maximal ideal. The following are equivalent.

  (1) R is a local ring with unique maximal ideal M.

  (2) $R \setminus R^\times$ is an ideal ($R^\times$ is the set of invertible elements of R).

  (3) There is a maximal ideal M of R such that $1 + m \in R^\times, \forall m \in M$.

- Noetherian: A commutative ring R is Noetherian or satisfy the ascending chain condition on ideals (or A.C.C) if whenever

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

  is an increasing chain of ideals of R, $\exists m \in \mathbb{N}$ such that $I_k = I_m, \forall k \geq m$. The following are equivalent.

  (1) R is a Noetherian ring.

  (2) Every nonempty set of ideals of R contains a maximal element (under inclusion).

  (3) Every ideal of R is finitely generated.

  We have analogous definitions and results for modules (submodules will be in place of ideals).

Problem 1.3. Let $\mathbb{F}_2$ be the field with 2 elements and let $R = \mathbb{F}_2[x]$. List, up to isomorphism, all R–modules of order 8.

Solution: First note that R is a P.I.D. since $\mathbb{F}_2$ is a field. By the Fundamental Theorem of Finitely Generated Modules over a P.I.D. I, we know that a finite R–module looks like

$$R/(a_1(x) \oplus R/a_2(x) \oplus \dots \oplus R/a_m(x),$$

where $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$. If $a(x)$ has degree n and we view $R/(a(x))$ as a R–vector space in the natural way (i.e. $r(\overline{f}) = \overline{rf}$), then we see that

$$\{\overline{1}, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}}\}$$

is a basis (linear independence comes from the fact that $\overline{f(x)} = 0$ in $R/(a(x))$ if and only if $f(x) \mid a(x)$. These elements span since $\overline{a(x)} = 0$ and so $\overline{x}^n$ can be written as a R–linear combination of the n elements. Higher powers of x can be dealt with by dividing by $a(x)$). Therefore (since $\mathbb{F}_2$ has 2 elements) we see that $R/(a(x))$ has 2^n elements.

Applying this to our current situation, we see that it must be the case that

$$\deg(a_1(x)) + \deg(a_2(x)) + \ldots + \deg(a_m(x)) = 3,$$

since $2^3 = 8$. There are 8 polynomials of degree 3 over $\mathbb{F}_2$, which gives us 8 possibilities:

$$R/(x^3), R/(x^3 + x^2), R/(x^3 + x), R/(x^3 + 1),$$

$$R/(x^3 + x^2 + x), R/(x^3 + x^2 + 1), R/(x^3 + x + 1), R/(x^3 + x^2 + x + 1).$$

There are 4 polynomials of degree 2 and 2 polynomials of degree 1:

$$x^2, x^2 + x, x^2 + 1, x^2 + x + 1;$$

$$x, x + 1.$$

From these we have that

$$x \mid x^2, x \mid x^2 + x, (x + 1) \mid x^2 + x.$$

This gives us 5 more possibilities:

$$R/(x) \oplus R/(x^2), R/(x) \oplus R/(x + x^2);$$

$$R/(x) \oplus R/(x) \oplus R/(x), R/(1 + x) \oplus R/(1 + x) \oplus R/(1 + x).$$

This gives us a total of 13 possible R–modules of order 8 over $\mathbb{F}_2$. By the uniqueness statement of the Fundamental Theorem, these are all distinct up to isomorphism. □

- Field: A field is a ring F with 1 such that $(F \setminus \{0\}, \cdot)$ is also an abelian group.
- Integral Domain: A commutative ring with identity $1 \neq 0$ is an integral domain if it has no zero divisors (i.e. no element r such that there is a non–zero element s with $rs = 0$).

- Principal Ideal Domain (P.I.D.): A principle ideal domain is an integral domain in which every ideal is principal, i.e. generated by a single element.

- $F[x] \Leftrightarrow$ P.I.D.: Let F be a commutative ring. Then $F[x]$ is a P.I.D. if and only if F is a field. (For the forward direction, prove the Division Algorithm for $F[x]$, i.e. if $a(x), b(x) \in F[x]$, then there exists unique $q(x), r(x) \in F[x]$ such that

$$a(x) = q(x)b(x) + r(x), \quad \text{with } r(x) = 0 \text{ or } \deg(r(x)) < \deg(b(x)).$$

  For the converse, notice that $F[x]/(x) \cong F$, which is a domain since $F[x]$ is, so that $(x) \subset F[x]$ is a prime, hence maximal ideal since $F[x]$ is a P.I.D).

- Fundamental Theorem of Finitely Generated Modules over a P.I.D I: Let R be a P.I.D. and let M be a finitely generated R–module. Then

$$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

  for some $r \in \mathbb{N} \cup \{0\}$ and $a_1, a_2, \ldots, a_m \in R$ such that

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

  The number r is called the free rank of M and the elements $a_1, a_2, \ldots, a_m \in R$ are called the invariant factors of M. Two finitely generated R–modules are isomorphic if and only if they have the same free rank and the same list of invariant factors.

- $F[x]/(a(x))$ as F–Vector Space: Let F be a field and let $a(x) \in F[x]$ be a polynomial of degree n. Then

$$\{\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}\}$$

  is an F–basis for $F[x]/(a(x))$ viewed as a vector space over F in the natural way. I.e. if $r \in F$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_1 x + a_0 \in F[x]$ and $\cdot$ represents the action of F on $F/(a(x))$, then

$$\begin{aligned} r \cdot \overline{f(x)} &= r \cdot \overline{(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)} \\ &= r \cdot (a_n \overline{x^n} + a_{n-1}\overline{x^{n-1}} + \cdots + a_1 \overline{x} + a_0) \\ &= r \cdot (a_n \overline{x}^n + a_{n-1}\overline{x}^{n-1} + \cdots + a_1 \overline{x} + a_0) (= r \cdot f(\overline{x})) \\ &= r a_n \overline{x}^n + r a_{n-1}\overline{x}^{n-1} + \cdots + r a_1 \overline{x} + r a_0 \\ &= (rf)(\overline{x}), \end{aligned}$$

  where the second and third equalities come from the fact that if $r \in F$, then

$$\overline{r x^m} = r x^m + (a(x)) = r(x^m + (a(x))) = r\overline{x^m}$$

  and

$$\overline{x^m} = x^m + (a(x)) = (x + a(x))^m = \overline{x}^m.$$

2 Winter 2002 – Rings

Problem 2.1. Let F be a field and A be a commutative F–algebra. Suppose A is of finite dimension as a vector space of F.

(a) Prove all prime ideals of A are maximal. Hint: consider maps $A/P \to A/P$ (P prime) of the form $x \mapsto ax$ with a in A.

(b) Prove that there are only finitely many maximal ideals of A.

Solution: (a) Let $\mathcal{B} \equiv \{\overline{x_1}, \overline{x_2}, \ldots, \overline{x_m}\}$ be a basis for A/P (A/P is finite dimensional since it is clear that $\{\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}\}$ spans A/P if $\{x_1, x_2, \ldots, x_n\}$ is a basis for A over F). Let $a \in A \setminus P$ and consider the map

$$\lambda_a : A/P \longrightarrow A/P : \overline{x} \mapsto a\overline{x} = \overline{a}\,\overline{x}.$$

P is a prime ideal so R/P is a domain, therefore λ_a is injective ($a\overline{x} = a\overline{y} \Leftrightarrow \overline{a}(\overline{x} - \overline{y}) = 0 \Leftrightarrow \overline{x} = \overline{y}$). We claim that $a\mathcal{B} \equiv \{a\overline{x_1}, a\overline{x_2}, \ldots, a\overline{x_m}\}$ is a basis for A/P: by injectivity all these elements are non–zero and distinct. Next suppose $\alpha_1, \alpha_2, \ldots, \alpha_m \in F$ are such that

$$\alpha_1 a\overline{x_1} + \alpha_2 a\overline{x_2} + \cdots + \alpha_m a\overline{x_m} = 0.$$

This implies that $\alpha_i a = 0, 1 \leq i \leq m$. Since $a \neq 0$, we must have $\alpha_i = 0, 1 \leq i \leq m$. So we conclude that $a\mathcal{B}$ is a linearly independent set over F. By the invariance of dimension property it must also be the case that this is a spanning set (if it were not, then we can throw in some $\overline{x}$ and still have linear independence, but then we would end up with a basis with more than m elements) and we conclude it is a basis.

From this we conclude that in fact λ_a is onto ($f_1 a\overline{x_1} + \cdots + f_m a\overline{x_m} = \lambda_a(f_1\overline{x_1} + \cdots + f_m a\overline{x_m})$ since A is commutative) and therefore $\exists \overline{x}$ such that $\overline{a}\,\overline{x} = \overline{1}$. This implies $\overline{x} = (\overline{a})^{-1}$ since A/P is a domain (dropping the bars, we have $ax = 1$ so $xax - x = (xa - 1)x = 0$, which implies $xa - 1 = 0$ and hence $xa = 1$ since $x \neq 0$). Since this holds for all $a \in A \setminus P$ ($\Leftrightarrow \overline{a} \neq \overline{0}$), we find that A/P is a field and hence P is maximal.

(b) First notice that any ideal of A is also a vector subspace of A. Next we claim A is Artinian (in fact also Noetherian): Let $I \subsetneq J$ be ideals of A. Since they are both subspaces of A it must be the case that the dimension of J is strictly greater than that of I (let $\mathcal{B} \equiv \{x_1, x_2, \ldots, x_n\}$ be a basis of I, then it must be the case that there is an element in $y \in J$ which does not lie in the F–span of $\mathcal{B}$. Then we see that $\mathcal{B} \cup \{y\}$ is part of a basis for J). Therefore any chain of ideals can have at most $\dim_F(A) + 1$ terms and hence is finite.

The result now follows from the fact that an Artinian ring can have only finitely many maximal ideals: Let $\mathcal{C}$ be the set of all ideals that can be written as an intersection of maximal ideals of A. Since A is Artinian, $\mathcal{C}$ has a minimal element $M \equiv M_1 \cap M_2 \cap \cdots \cap M_n$. Let N be a maximal ideal which is not one of $M_1, \ldots, M_n$. By the minimality of M,

$N \cap M = M$ and hence $M \subset N$. We claim that this implies $M_k \subset N$ for some $1 \leq k \leq n$: Let $k-1$ be the largest number such that $\tilde{M}_{k-1} \subsetneq N$, where $\tilde{M}_{k-1}$ is the intersection of all M_j for $j \leq k-1$ (if $k-1=0$, then $M_1 \subset N$). Let $x \in \tilde{M}_{k-1} \setminus N$. For all $y \in M_k$, $xy \in \tilde{M}_{k-1}M_k \subset \tilde{M}_{k-1} \cap M_k \subset N$ (by the maximality of $k-1$), so since N is maximal and hence prime, this implies $y \in M_k$. This holds for all $y \in M_k$ so $M_k \subset N$. Since M_k is a maximal ideal, $M_k = N$ and therefore $M_1, \ldots, M_n$ are all the maximal ideals of A. $\square$

- Algebra: An algebra is a set A over a field F such that
  - A is a vector space with respect to addition and multiplication by elements of the field.
  - A is a ring with respect to addition and multiplication.
  - $(\lambda a)b = a(\lambda b) = \lambda(ab)$ for any $\lambda \in F$, $a, b \in A$.

  Ideals of the ring A are the same as the ideals of the algebra A. If $I \subset A$ is an ideal, then I is also a subspace of the vector space A over F.
- Basis: Let V be a vector space. $\{e_1, e_2, \ldots, e_n\}$ is basis of V if any of the following equivalent conditions are satisfied:
  - Every $v \in V$ can be uniquely expressed as a linear combination of $e_1, e_2, \ldots, e_n$.
  - It is a set of linearly independent vectors that span.
  - It is a maximal linearly independent set and a minimal spanning set.
- Invariance of Dimension Property: If V is a finite–dimensional vector space, then any two bases of V have the same (finite) number of elements.
- Prime Ideal: Let R be a ring. A proper ideal $P \subset R$ is a prime ideal if given $a, b \in R$

$$ab \in P \Longrightarrow a \in P \text{ or } b \in P.$$

- P Prime $\Leftrightarrow$ R/P a Domain: Let R be a commutative ring. $P \subset R$ is a prime ideal if and only if R/P is an integral domain (i.e. has no zero divisors).
- M Maximal $\Leftrightarrow$ R/M a Field: Let R be a commutative ring. $M \subset R$ is a maximal ideal if and only if R/M is a field (use the Correspondence Principle and the fact that a commutative ring is a field if and only if it has no non–trivial ideals).
- Ideal $\rightsquigarrow$ Subspace: Let F be a field and R a finitely generated algebra over F. Then an ideal of R is also a vector subspace of R (viewed over F).

- Artinian: Let R be a commutative ring. R is Artinian or satisfy the descending chain condition (D.C.C.) if whenever

$$I_1 \supset I_2 \supset I_3 \supset \dots$$

is a decreasing chain of ideals of R, then there is some $m \in \mathbb{N}$ such that $I_k = I_m, \forall k \geq m$. Similarly for an R–module, with submodules replacing ideals. The following are equivalent.

(1) R is an Artinian ring.

(2) Every nonempty set of ideals of R contains a minimal element under inclusion.

  - An Artinian ring has only finitely many maximal ideals.
  - A finite dimensional algebra over a field is both Noetherian and Artinian.

- $A \cap B \subset P \Rightarrow A \subset P$ or $B \subset P$: Let R be a commutative ring. Let $A, B \subset R$ be ideals and suppose P is a prime ideal such that $A \cap B \subset P$. Then $A \subset P$ or $B \subset P$.

Problem 2.2. Let $A = M_n(F)$ be the ring of $n \times n$ matrices with entries in an infinite field F for $n > 1$. Prove the following facts:

(a) There are only 2 two–sided ideals of A;

(b) There are infinitely many maximal left ideals of A. Hint: Show that $Ax = Ay (x, y \in A)$ if and only if $\mathrm{Ker}(x) = \mathrm{Ker}(y)$.

Solution: (a) Suppose I is an ideal of A. We claim that the set of entries of matrices in I form an ideal in F: Let E_{ij} denote the matrix with the ij^{th} entry equal to 1 and the rest of the entries equal to zero. If $\alpha \in I$, then $E_{ij}\alpha E_{ij} = \alpha_{ij}E_{ij}$, where α_{ij} is the ij^{th} entry of α. By interchanging rows and columns (which correspond to multiplying by appropriate matrices in A: On the left (for rows) or right (for columns) by the matrix obtained from the identity matrix by interchanging the appropriate rows or columns), we can transform $\alpha_{ij}E_{ij}$ into $\alpha_{ij}E_{11}$. This shows that for each element x that shows up as an entry of a matrix in I, $xE_{11} \in I$. Since $xE_{11}yE_{11} = xyE_{11}$ and $xE_{11} + yE_{11} = (x+y)E_{11}$, we see that the set of entries of matrices of I form an ideal $I_F \subset F$.

Now we can set up a natural map

$$\lambda : \{\text{ideals of } A\} \longrightarrow \{\text{ideals of } F\} : I \mapsto I_F.$$

λ is clearly onto since given $J \subset F$ an ideal, $M_n(J) \subset M_n(F)$ is an ideal. We claim that λ is also 1-1: Suppose $I \neq I' \subset M_n(F)$ are ideals. By the operations described above, given any $x \in I_F$, $xE_{ij} \in I, \forall 1 \leq i, j \leq n$. Adding such xE_{ij}'s together, we may form any element of $M_n(I_F)$. Conversely it is clear that $I \subset M_n(I_F)$ and therefore $I = M_n(I_F)$. Similarly, $I' = M_n(I'_F)$. We conclude $M_n(I_F) \neq M_n(I'_F)$ and so $I_F \neq I'_F$.

λ is therefore a bijection so the only two–sided ideals of A are 0 and A, corresponding to the only ideals of F, namely 0 and F (if $I \subset F$ is a non–zero ideal, then let $0 \neq x \in I$. Since F is a field, x is invertible, so then $x^{-1} \cdot x = 1 \in I$ which implies that $I = F$).

(b)

- Ideals of $M_n(R)$: Let R be a ring with identity. Then every two–sided ideal of $M_n(R)$ is equal to $M_n(J)$ for some two–sided ideal $J \subset R$.
- Some Matrix Operations: Let R be a ring with identity. Let $E_{ij} \in M_n(R)$ be the matrix with the ij^{th} equal to 1 and all other entries equal to 0. Let I denote the identity matrix.
  - Let $A \in M_n(R)$. Then $E_{ij}AE_{ij} = a_{ij}E_{ij}$, where a_{ij} is the ij^{th} entry of A.
  - There are three elementary row and column operations:
    - Interchanging two rows or columns.
    - Adding a multiple of one row or column to another.
    - Multiplying any row or column by an element of $R^\times$.
  - Applying a row [column] operation α [β] to A corresponds to multiplying A on the left [right] by the (invertible) matrix obtained from I by applying the operation to I, i.e. $\alpha(A) = \alpha(I) \cdot A$ [$\beta(A) = A \cdot \beta(I)$].
- Ideals and Fields: If F is a field, then the only ideals of F are 0 and F.

Problem 2.3. Let $\mathbb{F}_2$ be the field with 2 elements and $A = \mathbb{F}_2[T, \frac{1}{T}]$ for an indeterminate T. Prove the following facts:

(a) The group of units in A is generated by T.

(b) There are infinitely many distinct ring endomorphisms of A.

(c) The ring automorphism group $\mathrm{Aut}(A)$ is of order 2.

Solution: (a) First observe that every element of A can be written as $\frac{f}{T^m}$, for some $f \in \mathbb{F}_2[T], m \in \mathbb{N}$: A generic element looks like

$$a_{-m}T^{-m} + a_{-(m-1)} \cdots + a_0 + a_1T + \cdots + a_nT^n.$$

Multiplying and dividing by T^m, we can write this as

$$\frac{a_{-m} + a_{-(m-1)}T + \cdots + a_0T^m + a_1T^{m+1} + \cdots + a_nT^{m+n}}{T^m}.$$

Now suppose $\frac{f}{T^m}$ is a unit A. Then $\frac{f}{T^m}\frac{g}{T^n} = \frac{fg}{T^{m+n}} = 1$ for some $\frac{g}{T^n} \in A$. So then $fg = T^{m+n}$, which implies that $f = T^l$, $l \in \mathbb{Z}$. So each element of $A^\times$ is some power (positive or negative) of T and hence T generates $A^\times$ as an infinite cyclic group.

(b) Consider the map $T \mapsto T^n$, for some $n \in \mathbb{Z}$. This can be extended to some map $\phi_n : A \longrightarrow A$ as follows: For all $a, b \in \mathbb{F}_2$, $m, m' \in \mathbb{Z}$, let

$$\phi_n(aT^m + bT^{m'}) = a\phi_n(T)^m + b\phi_n(T)^{m'} = aT^{nm} + bT^{nm'}, m \in \mathbb{Z}.$$

By construction ϕ_n is an endomorphism. If $n \neq m$, then $\phi_n \neq \phi_m$ (e.g. the images of T are not the same) and hence there are infinitely many endomorphisms since there are infinitely many integers.

(c) Let ϕ be an automorphism. Then ϕ maps a unit to a unit (if $x \in A$ is a unit, then $\phi(x) \cdot \phi(x^{-1}) = \phi(x \cdot x^{-1}) = \phi(1) = 1$, so $\phi(x)^{-1} = \phi(x^{-1})$). So in particular ϕ must be a group automorphism of $A^\times = \langle T \rangle \cong (\mathbb{Z}, +)$, by part (a) (the isomorphism is given by $T \mapsto 1 \in \mathbb{Z}$). We claim the automorphism group of $\mathbb{Z}$ has only 2 elements, given by $1 \mapsto 1$ and $1 \mapsto -1$: Suppose $\phi \in \mathrm{Aut}(\mathbb{Z})$ and $\phi(1) = n \in \mathbb{Z}$. Then

$$(n-1)\phi^{-1}(1) = \phi^{-1}(n-1) = \phi^{-1}(n) - \phi^{-1}(1) = 1 - \phi^{-1}(1),$$

so $1 = n\phi^{-1}(1)$, which implies $n = \pm 1$ since $\phi^{-1}(1)$ is an integer. So we conclude the only automorphisms of $\langle T \rangle$ are given by $T \mapsto T$ and $T \mapsto \frac{1}{T}$ and these clearly extend to be automorphisms of A. □

- $\mathrm{Aut}(\mathbb{Z})$: The automorphism group of $(\mathbb{Z}, +)$ has exactly two elements, given by $1 \mapsto 1$ and $1 \mapsto -1$.

3 Fall 2002 – Ring Theory

Problem 3.1. Let R be a commutative ring with 1, and let $S = R[x]$ be the polynomial ring in one variable. Suppose M is a maximal ideal of S. Prove that M cannot consist entirely of 0–divisors. Hint: You may want to distinguish the cases $x \in M$ and $x \notin M$.

Solution: First suppose $x \in M$. Suppose $f \cdot x = 0$ for some $f = a_n x^n + \cdots + a_1 x + a_0 \in S$. Then $a_i = 0, \forall 1 \leq i \leq n$ so $f = 0$ and we conclude x cannot be a 0–divisor. Now suppose $x \notin M$. M is maximal so S/M is a field. Therefore there exists some $\overline{f}$ such that $\overline{x}\overline{f} = \overline{1}$. Hence $xf + M = 1 + M$ and so $xf - 1 \equiv g \in M$. Suppose towards a contradiction that g were a 0–divisor. Then there exists some $0 \neq h \in S$ such that $xfh - h = gh = 0$. But then $xfh = h$, so that $h = 0$ since $\deg(xfh) \geq \deg(h) + 1$, a contradiction. □

Problem 3.2. Let R be a commutative ring with 1, and suppose I and J are ideals of R so that: $I + J = R$. Show that:

(i) $IJ = I \cap J$.

(ii) $R/IJ \cong R/I \oplus R/J$.

Solution: (i) First it is clear that $IJ \subset I \cap J$ (since ideals are closed under multiplication). Conversely suppose $a \in I \cap J$. Since $I + J = R$, there exists $x \in I, y \in J$ such that $x + y = 1$. Therefore $a = a(x + y) = ax + ay = xa + ay \in IJ$, since R is commutative.

(ii) Let

$$\phi : R \longrightarrow R/I \oplus R/J : r \mapsto (r + I, r + J).$$

Then ϕ is surjective homomorphism: That ϕ is a homomorphism is clear. To see that ϕ is surjective, note that since $I + J = R$, $\exists x \in I, y \in J$ such that $x + y = 1$. Then

$$(0 + I, x + J) + (y + I, 0 + J) = \phi(x) + \phi(y) = \phi(x + y) = \phi(1) = (1 + I, 1 + J).$$

So it must be the case that $\phi(x) = (0 + I, 1 + J)$ and $\phi(y) = (1 + I, 0 + J)$. Now if $(r + I, s + J) \in R/I \oplus R/J$ is arbitrary, then

$$\phi(xs+yr) = \phi(x)\phi(s)+\phi(y)\phi(r) = (0+I, 1+J)(s+I, s+J)+(1+I, 0+J)(r+I, r+J) = (r+I, s+J).$$

So we see that ϕ is surjective. Next,

$$\ker(\phi) = \{r \in R \mid r \in I, r \in J\} = I \cap J.$$

So by the First Isomorphism Theorem,

$$R/(I \cap J) \cong R/I \oplus R/J.$$

By (i), $I \cap J = IJ$, so $R/IJ \cong R/I \oplus R/J$. □

- Product of Ideals: Suppose I and J are ideals of a commutative ring R. Then IJ is the ideal consisting of all finite sums of elements of the form $xy, x \in I, y \in J$.
- Chinese Remainder Theorem: Let A_1, A_2 be ideals of a commutative ring (with 1) R. If A_1 and A_2 are comaximal (i.e. $A_1 + A_2 = R$), then $A_1 \cap A_2 = A_1A_2$ and

$$R/(A_1A_2) = R/(A_1 \cap A_2) \cong R/A_1 \times R/A_2.$$

  - This generalizes to the case of more ideals $A_1, A_2, \ldots, A_k$ under the condition that for all $i \neq j$, A_i and A_j are comaximal.
  - An application of this gives us the following: Let n be a positive integer with factorization $p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

    as rings so that in particular

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times.$$

– From the last equation we learn that ϕ is multiplicative, where ϕ is the Euler–ϕ function (counts the number of integers less than n that are relatively prime to n). Clearly $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ for p prime. Using these two facts we can determine the value of ϕ for any (positive) integer.

Problem 3.3. Let R be a commutative ring with 1, and let $S = R[x]$ be the polynomial ring in one variable. Let $f \in S$. If f is a unit of S (that is, f is invertible in S), show that f has the form $f = u + g$ where u is a unit in R and $g \in S$ is a nilpotent element without constant term.

Solution: Let $P \subset R$ be a prime ideal. Reduce all coefficients of f modulo P. Since $f \in (R[x])^\times$, $\overline{f} \in (\overline{R}[x])^\times$ ($\exists g \in S$ such that $gf = 1$, reducing modulo P, we get that $\overline{g}\,\overline{f} = \overline{1}$). Say $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then it must be the case that

$$a_i \in P, 1 \leq i \leq n \text{ and } a_0 \in \overline{R}^\times$$

since $\overline{R}$ is a domain so the units of $\overline{R}[x]$ are exactly the units of $\overline{R}$. Since P was arbitrary, we conclude that $a_i \in \bigcap_{P \text{ prime}} P, 1 \leq i \leq n$ and $a_0 \notin P$ for any prime ideal P. This immediately implies that $a_0 \in R^\times$ since a_0 is not in any maximal ideal (maximal ideals are prime) hence not in any proper ideal of R (if $a_0 \notin R^\times$, then $a_0 \in (a_0) \subsetneq R$).

Next we claim that $\bigcap_{P \text{ prime}} P = \text{nil}(R)$, where

$$\text{nil}(R) = \{x \in R \mid x^n = 0, \text{ some } n \in \mathbb{N}\}$$

is the set of nilpotent elements of R. First suppose $x \in R$, then $\exists n \in \mathbb{N}$ such that $x^n = 0 \in P$ for any prime P. Since P is prime, $x^k \in P$ for some $k < n$. Supoose k is minimal such that $x^k \in P$. If $k > 1$, then $x \cdot x^{k-1} \in P$, but then either $x \in P$ or $k - 1 \in P$, contradicting the minimality of k, so $k = 1$ and $x \in P$. Conversely, suppose $x \notin \text{nil}(R)$. Let $\mathcal{F}$ be the family of all proper ideals not containing any power of x. $\mathcal{F} \neq \emptyset$ since $0 \in \mathcal{F}$. Chains in $\mathcal{F}$ have upper bounds (if $x^k \in I_j$ for any I_j in the chain $I_1 \subset I_2 \subset \ldots$ then x^k is also not contained in the union of them), so by Zorn's lemma there is a maximal element P. P must be prime, since if $xy \in P$ and $x, y \notin P$, then $x^n \in (x) + P$, $x^m \in (y) + P$ for some $m, n \in \mathbb{N}$ by the maximality of P. But then $x^{m+n} \in (xy) + P = P$, a contradiction. So $x \notin P$.

Finally, $g \equiv a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x$ is nilpotent in S: Let α_i be such that $a_i^{\alpha_i} = 0$. Let N be the maximum of $\alpha_i, 1 \leq i \leq n$. Then $g^{Nn} = (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x)^{Nn} = 0$ (each term in the expansion must have some coefficient $a_n^{\alpha_n} \ldots a_1^{\alpha_1}$ such that $\alpha_n + \cdots + \alpha_1 = Nn$, which implies that there is some α_i such that $\alpha_i \geq N$) and hence g is nilpotent. □

- Polynomial Ring of Domains: Let R be an integral domain and $p(x), q(x) \in R[x]$. Then we have

(1) $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$.

(2) $(R[x])^\times = R^\times$.

(3) $R[x]$ is an integral domain.

- Nilradical: Let R be a commutative ring. Then the nilradical of R is exactly the intersection of all prime ideals in R.
- Zorn's Lemma: If A is a nonempty partially ordered set in which every chain has an upper bound then A has a maximal element.
- Krull's Theorem: Let R be a ring. Let $A \subset R$ be an ideal and $S \subset R$ a multiplicative set (a multiplicative set is a set such that if $x, y \in S$ then $xy \in S$, e.g. the $R \setminus P$ for a prime ideal P is a multiplicative set). Suppose $A \cap S = \emptyset$. Then there exists a prime ideal P maximal with respect to $A \subset P$ and $S \cap P = \emptyset$.

4 Winter 2003 – Rings

Problem 4.1. Give an example of two integral domains A and B which contain a field F such that $A \otimes_F B$ is not an integral domain. Justify your answer. Hint: Take A to be the field of rational functions $\mathbb{F}_p(X)$ for the field $\mathbb{F}_p$ with p elements.

Solution: Consider the tensor product $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ viewed as an $\mathbb{R}$–algebra. Notice that

$$(i \otimes i)(i \otimes i) = i^2 \otimes i^2 = (-1) \otimes (-1) = (-1)1 \otimes (-1) = 1.$$

So that $[(i \otimes i) - (1 \otimes 1)][(i \otimes i) + (1 \otimes 1)] = 0$, with neither of the factors equal to zero. So $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is not an integral domain.

- Tensor Product: Let R be a commutative ring. Let M, N be modules over R. The tensor product of M and N over R, denoted $M \otimes_R N$, is the quotient of the free $\mathbb{Z}$–module on the set $M \times N$ by the subgroup generated by

  $$(m_1 + m_2, n) - (m_1, n) - (m_2, n), \quad (m, n_1 + n_2) - (m, n_1) - (m, n_2), \quad (mr, n) - (m, rn).$$

  We have the relations

  $$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n,$$

  $$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2,$$

  $$mr \otimes n = m \otimes rn.$$

– Notice that $0 \otimes n = m \otimes n = 0$ for any $m \in M, n \in N$.

– $M \otimes_R N$ is a left R–module such that if $r \in R$, then

$$r(m \otimes n) = (rm) \otimes n = m \otimes (rn).$$

– Universal Property of Tensor Products: If L is any left R–module, then there is a bijection

$$\left\{ \begin{array}{c} R\text{–bilinear maps} \\ \phi : M \times N \to L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} R\text{–module homomorphisms} \\ \Phi : M \otimes_R N \to L \end{array} \right\}$$

given by

$$\pi \circ \Phi = \phi,$$

where

$$\pi : M \times N \to M \otimes_R N : (m, n) \mapsto m \otimes n$$

is a bilinear map. This basically follows from the Universal Property of Free Modules: If A is a set and $F(A)$ is the free R–module on the set A (i.e. all elements of the form $r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$, for $r_i \in R, n \in \mathbb{N}$ such that each element of $F(A)$ has a unique expression of this form), then any map from A into a group G can be uniquely extended to a R–module homomorphism from $F(A)$ to G.

– If A and B are R–algebras, then

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'$$

is well–defined and makes $A \otimes_R B$ into an R–algebra.

– Notice that $R \otimes_R R \cong R$ and $(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N)$ and $M \otimes_R (N \oplus N') \cong (M \otimes_R N) \oplus (M \otimes N')$, so that if M, N are free with bases $m_1, \ldots, m_s$ and $n_1, \ldots n_t$ then $M \otimes_R N$ is free of rank st, with basis $m_i \otimes n_j, 1 \leq i \leq s, 1 \leq j \leq t$, i.e.

$$R^s \otimes_R R^t \cong R^{st}.$$

Problem 4.2. Let $\mathbb{F}_q$ be the finite field of q elements, and put $F = \mathbb{F}_q$ and $K = \mathbb{F}_{q^2}$. Write $\sigma : K \to K$ for the field automorphism given by $x^\sigma = x^q$. Let

$$B = \left\{ \left(\begin{array}{cc} a & b \\ db^\sigma & a^\sigma \end{array} \right) \middle| \; a, b \in K \right\}$$

for a given $d \in F^\times$. Prove the following three facts:

(a) B is a subalgebra of dimension 4 over F inside the F–algebra of 2×2 matrices over K.

(b) B is a division algebra if and only if there exists no $c \in K$ such that $d = cc^\sigma$.

(c) B cannot be a division algebra.

Solution: (a) Let $\{1, \alpha\}$ be a basis for K over F. Then

$$\mathcal{B} \equiv \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_a, \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^\sigma \end{pmatrix} = A_a, \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix} = I_b, \begin{pmatrix} 0 & \alpha \\ d\alpha^\sigma & 0 \end{pmatrix} = A_b \right\}$$

is a basis for B over F. Let $\mathrm{char}(K) = p$ and $q = p^n$, some n. To see that $\mathcal{B}$ spans, suppose $a = x + y\alpha$, $b = w + z\alpha$, $x, y, z, w \in F$, then

$$xI_a + yA_a + wI_b + zA_b = \begin{pmatrix} x + y\alpha & 0 \\ 0 & x + y\alpha^\sigma \end{pmatrix} + \begin{pmatrix} 0 & w + z\alpha \\ wd + zd\alpha^\sigma & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ db^\sigma & a^\sigma \end{pmatrix},$$

where the last equality comes from the fact that since $\mathrm{char}(K) = p$ and $\gamma^q = \gamma, \forall \gamma \in F$,

$$(x + y\alpha)^q = (x + y\alpha)^{p^n} = x^q + y^q\alpha^q = x + y\alpha^q$$

$(p \mid \binom{p^n}{k}, 1 \le k < p^n)$ and similarly $d(w + z\alpha)^q = d(w + z\alpha^q)$.

For linear independence first note that I_a and A_a are linearly independent over F since 1 and α are. I_b and A_b are both linearly independent from both I_a and A_a because of the position of 0's. Finally, I_b and A_b are linearly independent from each other again because 1 and α are linearly independent.

(b) First suppose there is some $c \in K$ such that $d = cc^\sigma = c^{q+1}$, then set $b = 1$ and $a = c$ and we get

$$A \equiv \begin{pmatrix} c & 1 \\ c^{q+1} & c^q \end{pmatrix} \in B.$$

Clearly $A \neq 0$ but $\det(A) = 0$ so A cannot be invertible and hence B is not a division algebra. Conversely suppose B is not a division algebra. Then $\exists a, b \in K$, not both equal to zero, such that $A \equiv \begin{pmatrix} a & b \\ db^q & a^q \end{pmatrix}$ is not invertible. This implies $\det(A) = a^{q+1} - db^{q+1} = 0$. If either a or b is equal to zero, then that forces the other to be 0 (since K has no zero divisors) and then $A \equiv 0$ so suppose $a, b \neq 0$. Then the equation says $a^{q+1} = db^{q+1}$, which implies $d = (ab^{-1})^{q+1} = ab^{-1}(ab^{-1})^\sigma$.

(c) By (b) it suffices to show that there is some $c \in K$ such that $cc^\sigma = c^{q+1} = d$. Consider the polynomial $f \equiv x^{q+1} - d$ over F. We claim that f has some root $c \in K$ (of course then $d = cc^\sigma$): $d \in F^\times$ so $d^{q-1} = 1$, so we have

$$x^{q+1} - d \mid (x^{q+1})^{q-1} - d^{q-1} = x^{q^2-1} - 1 \mid x^{q^2} - x = x^{p^{2n}} - x.$$

From this we conclude that there is a root of f in K since $|K| = q^2 = p^{2n}$ and hence K is the splitting field of $x^{p^{2n}} - x$. □

Problem 4.3. Let A be a discrete valuation ring with maximal ideal M, and define

$$B = \{(a, b) \in A \times A \mid a \equiv b \bmod M\}.$$

Prove the following facts:

(a) B has only one maximal ideal;

(b) B has exactly two non–maximal prime ideals.