MATH 435 ASSIGNMENT 4

ARNOLD JIADONG YU

1. Chapter 15 Ring Homomorphisms

1.1. Let $Z[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in Z\}$ and

$$H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \middle| a, b \in Z \right\}$$

Show that $Z[\sqrt{2}]$ and H are isomorphic as rings.
proof: Let f be a map such that

$$f : Z[\sqrt{2}] \to H$$

$$f : (a + \sqrt{2}b) \mapsto \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}, \text{ where } a \in Z, b \in Z$$

Pick $a + \sqrt{2}b, c + \sqrt{2}d \in Z[\sqrt{2}]$, then $f(a + \sqrt{2}b) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ and $f(c + \sqrt{2}d) = \begin{bmatrix} c & 2d \\ d & c \end{bmatrix}$.

$$f(a + \sqrt{2}b) + f(c + \sqrt{2}d) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix}$$

$$= \begin{bmatrix} a + c & 2(b + d) \\ b + d & a + c \end{bmatrix} = f((a + c) + \sqrt{2}(b + d))$$

$$f(a + \sqrt{2}b) \cdot f(c + \sqrt{2}d) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & 2d \\ d & c \end{bmatrix}$$

$$= \begin{bmatrix} ac + 2bd & 2ad + 2bc \\ ad + bc & ac + 2bd \end{bmatrix} = f((ac+2bd)+\sqrt{2}(ad+bc)) = f((a+\sqrt{2}b)\cdot(c+\sqrt{2}d))$$

Therefore, f is ring homomorphism. Let $f(a + \sqrt{2}b) = f(c + \sqrt{2}d)$, then

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} = \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \Rightarrow a = c, b = d \Rightarrow a + \sqrt{2}b = c + \sqrt{2}d$$

Therefore, f is injective function. Let $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$, then $f(a+\sqrt{2}b) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$, which means for $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \in H$, there exists $a+\sqrt{2}b \in Z[\sqrt{2}]$. Therefore, f is also surjective. Hence, f is bijective. As a result, $Z[\sqrt{2}]$ and H are isomorphic as rings.

2. Chapter 14 Ideal and Factor Rings

2.1. If A and B are ideals of a ring, show that the *sum* of A and B, $A+B = \{a+b | a \in A, b \in B\}$, is an ideal.
proof: Let R be a ring, and A, B are ideals of R. i.e. A, B are normal subgroup under addition, for any $a, c \in A, b, d \in B$, $a-c \in A, b-d \in B$ and any $r \in R$, $ar \in A, ra \in A$ and $br \in B, rb \in B$.
(1) For $a+b, c+d \in A+B$, $(a+b)-(c+d) = (a-c)+(b-d) \in A+B$ since $a-c \in A, b-d \in B$ and addition is associative.
(2) For $a+b \in A+B$ and $r \in R$. $r(a+b) = ra+rb \in A+B$ since $ra \in A, rb \in B$. Moreover, $(a+b)r = ar+br \in A+B$ since $ar \in A, br \in B$. Hence $A+B$ is an ideal by Ideal Test.

2.2. If A and B are ideals of a ring, show that the *product* of A and B, $AB = \{a_1b_1 + a_2b_2 + ... + a_nb_n | a_i \in A, b_i \in B, n \text{ a positive integer }\}$, is an ideal.
proof: Let R be a ring, and A, B are ideals of R. i.e. A, B are normal subgroup under addition, for any $a_i, c_i \in A, b_i, d_i \in B$, $a_i - c_i \in A, b_i - d_i \in B$ and any $r \in R$, $a_ir \in A, ra_i \in A$ and $b_ir \in B, rb_i \in B$.
(1) For $a_1b_1 + ... + a_nb_n, c_1b_1 + ... + c_mb_m \in AB$. WLOG, assume $n > m$

$$(a_1b_1 + ... + a_nb_n) - (c_1b_1 + ... + c_mb_m)$$
$$= a_1b_1 - c_1b_1 + ... + a_mb_m - c_mb_m + a_{m+1}b_{m+1} + ... + a_nb_n$$
$$= (a_1 - c_1)b_1 + ... + (a_m - c_m)b_m + a_{m+1}b_{m+1} + ... + a_nb_n \in AB$$

Since , $a_i, a_i - c_i \in A, b_i \in B$.
(2) For $a_1b_1 + ... + a_nb_n \in AB$ and $r \in R$,

$$(a_1b_1+...+a_nb_n)r = (a_1b_1)r+...+(a_nb_n)r = a_1(b_1r)+...+a_n(b_nr) \in AB$$

Since R is associative respect to multiplication and $a_i \in A, b_ir \in B$.

$$r(a_1b_1+...+a_nb_n) = r(a_1b_1)+...+r(a_nb_n) = (ra_1)b_1+...+(ra_n)b_n \in AB$$

Since R is associative respect to multiplication and $ra_i \in A, b_i \in B$. Hence AB is an ideal by Ideal Test.

2.3. *Does the previous exercise work if you define the product of ideals as $A \times B = \{ab|a \in a, b \in B\}$? Prove or give a counterexample.
proof:

2.4. Show that $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field.
proof: WTS $\langle x^2+1\rangle$ is maximal ideal.
$\langle x^2+1\rangle$ is a principal ideal since $\langle x^2+1\rangle = \{f(x)(x^2+1)|f(x) \in \mathbb{R}[x]\}$. Let I be ideal of R, s.t. $\langle x^2+1\rangle \subsetneq I \subseteq \mathbb{R}[x]$. WTS $I = \mathbb{R}[x]$, it is same to show $1 \in I$.

$$\mathbb{R}[x]/\langle x^2+1\rangle = \{ax+b+\langle x^2+1\rangle | a, b \in \mathbb{R}\}$$

Let $f(x) \in I \setminus \langle x^2+1\rangle$, then $f(x) \in \mathbb{R}[x]$, i.e. $f(x) = q(x)(x^2+1)+r(x)$, where $q(x) \in \mathbb{R}[x], r(x) = ax+b \neq 0$. Since it is for all $x \in \mathbb{R}$, then a, b can not be both zero. Moreover, $ax+b \in I$ when $g(x) = 0$. Let $cx+d \in I$ s.t. $(ax+c)(cx+d) = 1$, if such $cx+d$ exists, then $1 \in I$. Therefore,

$$(ax+b)(cx+d) = acx^2+(ad+bc)x+bd = ac(x^2+1)+(ad+bc)x+bd-ac = 1$$

$$\Rightarrow ad+bc = 0, bd-ac = 1$$

By solving the equations, we obtain $c = \frac{-a}{a^2+b^2}, d = \frac{b}{a^2+b^2}$. Such c, d exists since $a^2+b^2 \neq 0$. That is $1 \in I$, this implies $I = \mathbb{R}[x]$. Hence $\langle x^2+1\rangle$ is a maximal ideal. As a result, $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field.

2.5. * Let R be a commutative ring and let A be any ideal of R. Show that the *nil radical* of A, $N(A) = \{r \in R | r^n \in A$ for some positive integer n(n depends on r)$\}$, is an ideal of R. [$N(\langle 0\rangle)$ is called the *nil radical* of R.]

2.6. In a principal ideal domain, show that every nontrivial prime ideal is a maximal ideal.
proof: Let R be a principal ideal domain, and I be an nontrivial prime ideal, then there exists an $a \in R$ s.t. $I = \langle a\rangle$. Assume there exists another ideal J, s.t. $I \subsetneq J \subseteq R$. Then $J = \langle b\rangle$ for some $b \in R$. Since $\langle a\rangle \subset \langle b\rangle$, then $a \in \langle b\rangle$ but $b \notin \langle a\rangle$. i.e. $a = bs$ for some $s \in R$. I is prime ideal and $bs \in \langle a\rangle$ implies $s \in \langle a\rangle$ since $b \notin \langle a\rangle$. Then $s = ta$ for some $t \in R$, then

$$a = bs, s = ta \Rightarrow a = bta$$

By cancellation, we obtain $bt = 1$. Since $bt \in \langle b\rangle$, then $1 \in J$, this implies $J = R$. Hence I is also maximal ideal.

2.7. Suppose that R is a commutative ring with unity such that for each a in R there is a positive integer n greater than 1 (n depends on a) such that $a^n = a$. Prove that every prime ideal of R is a maximal ideal of R.
proof: Suppose that R is a commutative ring with unity and I be a prime ideal of R, then R/I is an integral domain. WTS R/I is also a field.
$a + I \in R/I$, and $(a + I)^n = a^n + I = a + I$. i.e. $[a^n] = [a]$ implies $[a^{n-1}] = [1]$ by cancellation. Moreover,$[a^{n-1}] = [a][a^{n-2}] = [1]$, i.e. the inverse of $a + I$ is $a^{n-2} + I$. Therefore, for every $a + I \in R/I$ have a multiplicative inverse, i.e. $a + I$ is a unit. Hence R/I is a field, and furthermore I is a maximal ideal.