MTH 316 Homework 1

Evan Fox (efox20@uri.edu)

July 12, 2022

Theorem 1.
1. *Let $u \in R$, u is a left unit if and only if left multiplication by u is surjective*
2. *If u is a left unit, then right multiplication by u is injective*
3. *A two-sided unit is unique*
4. *The two sided units of R form a group*

Proof. For (1) first assume that u is a left unit of R. Then there exists $v \in R$ such that $uv = 1$. Then for $x \in R$ it we have

$$u(vx) = (uv)x = 1x = x$$

since multiplication is associative. Conversly, if left multiplication by u is surjective then there must exist $v \in R$ satisfying $uv = 1$ by the defintion of surjectivity. For (2) assume that $u \in R$ is a left unit. We want to show that right multiplcation by u is injective, i.e.

$$xu = yu \implies x = y$$

Since u is a left unit, we fix $v \in R$ satisfying $uv = 1$ then by right multiplying both sides of the above by v we get

$$x(uv) = y(uv)$$

$$x = y$$

For (3) let u be a two sided unit, then fix $v \in R$ such that $vu = uv = 1$. suppose v' is another inverse of u satisfying $uv' = 1$. Then, we have $uv = uv'$. multiplying on the left by v gives

$$vuv = vuv'$$

$$v = v'$$

and we are done. Note that we could fist prove that the two sided units for a group and then this result would follow. For (4) we need to show the four group axioms. Associativity follows from the fact that R is a ring. Now we show closure under multiplication. if u, v are two unints then uv is also a unit with inverse $(v^{-1}u^{-1})$. Since 1 is a unit (by definition) we have we have identity. and we know that the inverse of uv is a two sided unit with inverse uv.

□

Question 1.

Find a sutiable multiplication on $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ that turns it into a field.

Proof. We let $(1, 1)$ be the identity. Then let $(1, 0) * (0, 1) = (1, 1)$ and let the squares of $(1, 0)$ and $(0, 1)$ map to each other. We claim this gives a field. A routine verification shows this to be the case. A good follow up question is whether or not this multiplication is unique. □

Question 2.

prove that $\mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ forms a ring.

Proof. First we must show that it is an abelian group under addition, we let addition be defined as addition of real numebers, then associativity and communitivity follows. We see that $0 \in \mathbb{Z}(\sqrt{2})$ is the identity. And for any element $z \in \mathbb{Z}(\sqrt{2})$ with $z = a+b(\sqrt{2})$ the additive inverse is found by taking the inverses of a, b in the intergers. Clousre will follow by an application of the distributuive property.

Next we define multiplication in $\mathbb{Z}(\sqrt{2})$ as multiplication of real numbers, so associativity is clear. Then this ring clearly has unit by taking $a = 1, b = 0$. For $z, z' \in \mathbb{Z}(\sqrt{2})$ we have

$$z \cdot z' = (a + b\sqrt{2})(a' + b'\sqrt{2}) = aa' + 2bb' + (ab' + a'b)\sqrt{2}$$

so it is closed under multiplication. □

is $\mathbb{Z}(\sqrt{2})$ a intergral domain? is it a field? It is definily an intergral domain since the intergers are an intergral domain. is it a field? What would a multiplicitive inverse look like? We would need $ab' + a'b = 0$. Which is possible but then $aa\prime + 2bb' \neq 1$, so we do not get multiplicitive inverses. We know that each element has an inverse in $\mathbb{R}$ the question is can this be written in the form we are looking for? $\frac{1}{a+b\sqrt{2}}$ The question is can I prove that this cannot be written as $c+d\sqrt{2}$? Suppose that I can for all $a,b,c,d \in \mathbb{Z}$.

$$\frac{1}{a+b\sqrt{2}} = c+d\sqrt{2}$$

$$1 = ac+2bd+(ad+bc)\sqrt{2}$$

so

$$ac+2bd = 1 \text{ and } ad+bc = 0$$

Then we note that if a is even then $\gcd(a,2b) \neq 1$ and thus the existance of c and d gives a contradiction.

Theorem 2. *For $a,b,d \in \mathbb{Z}$ we have $\gcd(a,b) = d$ implies that there exists $s,t \in \mathbb{Z}$ which satisfy the equation $as+bt = d$.*

Proof. First assume that $\gcd(a,b) = d$. Then let $S = \{ax+by > 0 | x,y \in \mathbb{Z}$ $\}$. Since this is a subset of the natural numbers we can fix $\alpha = as+bt$ as the least element. We want to show that this is the GCD of a and b. First we show that if d' is a common divisor the $d'|\alpha$. Since d' is a common divisor we can write $dx = a$ and $dy = b$. Then

$$\alpha = as+bt = d'xs+dyt = d'(xs+yt)$$

hence $d'|\alpha$. Now we shoe that α itself is a common divisor, let

$$a = q_0\alpha + r_0 \text{ and } b = q_1\alpha + r_1$$

with $0 \leq r_0 < \alpha$ ad $0 \leq r_1 < \alpha$

$$a = q_0(\alpha) + r_0 = q_0(as+bt) + r_0$$

$$a - q_0as - q_0bt = r_0$$

$$a(1-q_0s) + b(-q_0t) = r_0$$

So that $r_0 = 0$ and then it follows that $\alpha|a$; a simillar argument works for b. So we have that α is a common divisor of a and b and that if d' is an arbitrary common divisor it divides α. It now follows that $\alpha = \gcd(a,b)$.

□

Corollary 2.1. *If $GCD(a,b) = 1$ then there exists $s,t \in \mathbb{Z}$ such that $as + bt = 1$.*

Corollary 2.2. *If there exists $s,t \in Z$ such that $as+bt = 1$ then $\gcd(a,b) = 1$.*

So now we know that $\mathbb{Z}(\sqrt{2})$ is not a field. But it is an intergral domain.

What else can I figure out about this ring. What are the ideals of this ring?

Let T be a ring without unit, then define $R = \mathbb{Z} \times T$ and define the operations of addition and multiplication on R as follows

$$(k,l) + (s,t) = (k+s, l+t)$$

and

$$(k,l) \cdot (s,t) = (ks, kt + sl + lt)$$

Theorem 3. *R as defined above is a ring with unit $1_R = (1_\mathbb{Z}, 0_T)$.*

Proof. Our first order of buisness is to prove that R forms a abelian group under addition.

1. $[(a,b)+(c,d)]+(e,f) = (a+c, b+d)+(e,f) = (a+c+e, b+d+f) = (a,b) + [(c,d)+(e,f)]$ the addition is associative.
2. $\mathbb{Z}$ and T are both groups so $(a,b)+(c,d) = (a+c, b+d) \in \mathbb{Z} \times T$.
3. $0_\mathbb{Z} \in \mathbb{Z}$ and $0_T \in T$ so $(0,0) + (a,b) = (0+a, 0+b) = (a,b)$; thus an additive identity exists.
4. For $(a,b) \in \mathbb{Z} \times T$ we have $-a \in \mathbb{Z}$ and $-b \in T$. Then $(a,b)+(-a,-b) = (a+(-a), b+(-b)) = (0,0)$
5. $\mathbb{Z}$ and T are rings so their addition commutes giving $(a,b)+(c,d) = (a+c, b+d) = (c+a, d+b) = (c,d)+(a,d)$

Now we show that the defined multiplication gives R a ring structure. The clousure of this operation follows from the fact that T and $\mathbb{Z}$ are rings. We first show that $(1_\mathbb{Z}, 0_T)$ is the multiplicitive identity. Let $(a,b) \in R$ and

$$(a,b) \cdot (1,0) = (1a, a(0) + 1b + b \cdot (0)) = (a,b)$$

and

$$(1,0) \cdot (a,b) = (1a, 1b + a(0) + 0 \cdot (b))$$

So we have a unit element. To see that the multiplication on R is associative.

$$[(a,b)\cdot(c,d)]\cdot(e,f) = (ac, ad+cb+b\cdot d)\cdot(e,f) =$$

$$= (ace, acf+ead+ecb+e(b\cdot d)+(ad+cb+b\cdot d)\cdot f)$$

and then

$$(a,b)\cdot[(c,d)\cdot(e,f)] = (a,b)\cdot(ce, cf+ed+d\cdot f) =$$

$$= (ace, acf+aed+a(d\cdot f)+ceb+b\cdot(cf+ed+d\cdot f))$$

and we can see that the product is associative. Lastsly we need to show that the distributive property holds. This will follow from the ring structure of T and the fact that addition was defined component wise. □

We say that this is an embedding of T into the ring R. By embedding a rint T into a larger ring with unit enables us to study the ring T more readily. What is presevered by this embedding? They are not isomophic since $|R| > |T|$.

conjectures:

1. communitivity
2. if the group structure of T is cyclic then so is R.
3. If U is an ideal of T then $U' = \{(0_{\mathbb{Z}}, x) | x \in U\}$ is an ideal in R.
4. $T \cong U = \{(0_{\mathbb{Z}}, x) | x \in T\}$ with $t \mapsto (0_{\mathbb{Z}}, t)$.

Theorem 4. *If R is a boolean ring i.e. ($x^2 = x$) for all x then R is communitive.*

Proof. Let $a, b \in R$ and we have $(a+b)^2 = a+b = a^2+b^2$. But by the distributive property we have $(a+b)^2 = a^2+ab+ba+b^2$. So we see

$$a^2+b^2 = a^2+ab+ba+b^2$$

$$ab = -ba$$

Now we prove that in a boolen ring every element has order 2 under addition.

$$2x = (2x)^2 = 4x^2 = 4x$$

which implies

$$0 = 2x$$

□

Let R be a ring with ideal I. Let $M_n(I)$ be a subset of the matrix ring $M_n(R)$ consisting on those matrices whose elements are in I. It is easy to check that this forms an ideal of the ring $M_n(R)$. Now prove that every ideal of $M_n(R)$ has this form.

Proof. First we check that $M_n(I)$ is an ideal. Associativity and communitivity of addition follows since these are matrices. Since the elements of the matrices in $M_n(I)$ are in I when we add to matrices component wise we get elements of the form $a+b$ for $a, b \in I$ and so $a+b \in I$. Hence all elements of the sum of two matrices are in I and so the sum of the matrices is in $M_n(I)$. This shows that we have an abelian group under addition. Now we need to show that it is closed under left and right multiplication by elements of R. Again since all elements in a given matrix $A \in M_n(I)$ are in an ideal, thier multiplication by any element of R must again be in I. The argument is very similiar to the first part of the proof.

Now let U be an ideal of $M_n(R)$. Let U' be the subset of R given by $x \in U'$ if x is an element of a matrix in U. Then, $a, b \in U'$ implies there exists a matrix A with $(A)_{1,1} = a$ and B such that $(B)_{1,1} = b$ Then the matrix $A+B$ contains $a+b$ so $a+b \in U'$. The rest of the group axioms follow in a similar manner. Then we must show that U' is closed under multiplication by elements of R. This again follows since for $a \in U$ we have $(A)_{1,1} = a$ and since U is an ideal of $M_n(R)$ we fix a matrix that has r in the 1,1 component. Then the mutplication of the matrices must be contained in the ideal U and it has entries ra so $ra \in U'$ when $a \in U'$. □

let $a^3 = a$ for all $a \in R$. Prove that R is communitive.

Proof.

$$a^2 + ab + ba + b^2(a+b) = a^3 + a^2b + aba + ab^2 + ba^2 + bab + b^2a + b^3$$

How do I show that a and b commute? □

Theorem 5. $\hom(\mathbb{Z}_n, \mathbb{Z}_m) = \mathbb{Z}_{\gcd(m,n)}$

The only ideals of a field are $\{0\}$ and the field itself.

Proof. Let U be an ideal of a field $\mathbb{F}$ and suppose that $U \neq \{0\}$. Then we may fix $a \in U$ such that $a \neq 0$. Since $\mathbb{F}^*$ forms a group we know there exists $a^{-1} \in \mathbb{F}$ and since U is an ideal it must be closed under multiplication by elements of $\mathbb{F}$. Hence $aa^{-1} = 1 \in \mathbb{F}$. Now we apply the same argument again, since U is closed under multiplication by elements of $\mathbb{F}$ for any $x \in \mathbb{F}$ we have $1 \cdot x = x \in U$; thus, $U = \mathbb{F}$. □

consider the quaternions with interger coefficents. Prove this forms a ring and that it's only ideals are $\{0\}$ and the ring itself. Then prove that the quaternions with interger coefficents do not form a field, they are not communitive!

$\mathbb{Z}_7[\sqrt{3}]$ is a field. determine necessary and sufficient conditions for $Z_p[\sqrt{k}]$ to be a field for prime p and integer k.

$$\frac{1}{a+b\sqrt{3}} \cdot \frac{a-b\sqrt{3}}{a-b\sqrt{3}} = \frac{a-b\sqrt{3}}{a^2-3b^2} =$$

maximal ideal: An ideal M is said to be maximal if and only for any ideal U such that $M \subseteq U$ we have $U = M$ or $U = R$. That is, M is a maximal ideal if it is impossible to fit an ideal between it and the entire ring. It is possible to have more than one maximal ideal.

Let $I = \langle 2 \rangle$ and note that this is a maximal ideal of $\mathbb{Z}$ but $I[x]$ is not a maximal ideal of $\mathbb{Z}[x]$.

Proof. Let $U \subseteq \mathbb{Z}$ an an ideal properly conatining $\langle 2 \rangle$. Then fix $a \in U$ with $a \notin \langle 2 \rangle$. Since $\gcd(a, 2) = 1$ we are permitted to fix $s, t \in \mathbb{Z}$ such that $sa + t2 = 1$. Then it since U is an ideal containg the identity it must be the ring itself. Now we want to find a proper ideal of $\mathbb{Z}[x]$ containing $I[x]$. Suppose $I[x] \subset U[x] \subseteq z[x]$. Then in particular, there exists a polynomial with odd coeficeint. □

A communitive ring with the cancellation property has no zero-divisors

Proof. Let R be communitive with cancellation. Then suppose $ab = 0$. We have

$$ab = 0b$$

□

$$f(x) = x^2$$

Let G be a cyclic group and $H \leq G$. Since G is cyclic, we have

$$G = \{g^{-1}, 0, g^1, g^2, \dots\} = \langle g \rangle$$

and H contains some subcollection of these elements. Let $S = \{a | a \in \mathbb{N}, g^a \in H\}$. Let s be the least element of S. Let $g^n \in H$ and use the division algrothim to fix $g, r \in \mathbb{Z}$ such that

$$n = qs + r \text{ with } 0 < r < s$$

Then since s is the least element of S greater than 0, $r = 0$.

$$g^n = g^{qs+r} = g^q s g^r = g^q s$$

so that every element of H is a multiple of g^s, so then $H = \langle g^s \rangle$.