John B Sec.26: Theorems and answers

Date: Jan 19 Made by Eric

Definition and Theorems

Theorem 1. *Let R and R' be two rings, where there exists a homomorphism $\phi : R \mapsto R'$. Let 0 be the additive identity of R, $\phi(0) = 0'$ is the additive identity od R', and if $a \in R$, then $\phi(-a) = -\phi(a)$. If S is a subring of R, then $\phi[S]$ is a subring of R'. If S' is a subring of R', then $\phi^{-1}[S']$ is a subring of R. If R have unity 1, $\phi(1)$ is the unity $\phi[R]$, where R' may or may not have the unity.*

Proof. Assume $\phi(0) \neq 0'$.

Let $r \neq 0 \in R, \phi(r) = \phi(r + 0) = \phi(r) + \phi(0) \neq \phi(r)$. OPID.

$\phi(-a) + \phi(a) = \phi(0) = 0' \implies \phi(-a) = -\phi(a)$. OPID.

$\forall \phi(s_1), \phi(s_2) \in \phi[S], \phi(s_1) + \phi(s_2) = \phi(s_1 + s_2) \in \phi[S], \phi(s_1)\phi(s_2) = \phi(s_1 s_2) \in \phi[S]$. $\phi[S]$ is closed under.

$0' = \phi(0) \in \phi[S]$, since $0 \in S$.

$\forall \phi(s) \in \phi[S], \exists \phi(-s) \in \phi[S]$.

$\phi(s) + \phi(-s) = \phi(0) = 0'$. Inverse included. OPID

Let $a, b \in \phi^{-1}[S']$.

$\phi(a + b) = \phi(a) + \phi(b) \in S' \implies a + b \in \phi^{-1}[S']$.

$\phi(ab) = \phi(a)\phi(b) \in S' \implies ab \in \phi^{-1}[S']$. $\phi^{-1}[S']$ is closed under.

$\phi(0) = 0' \in S', \implies 0 \in \phi^{-1}[S']$.

$\phi(-a) = -\phi(a) \in S' \implies -a \in \phi^{-1}[S]$. Inverse included. OPID.

$\forall \phi(r) \in \phi[R], \phi(r)\phi(1) = \phi(r)$. OPID.

The fact that R' may not have the unity is left **to prove**.

■

Theorem 2. *Let $\phi : R \mapsto R'$ be a ring homomorphism, where H=ker(ϕ). Let $a \in R$, then $\phi^{-1}[\phi(a)] = a + H = H + a$.*

Proof. $\forall a+h \in a+H, a+h = h+a \in H+a \implies a+H \subseteq H+a.$

$\forall h+a \in H+a, h+a = a+h \in a+H \implies H+a \subseteq a+H.$

$\implies a+H = H+a.$ OPID.

$\forall a+h \in a+H, \phi(a+h) = \phi(a)+\phi(h) = \phi(a) \implies a+h \in \phi^{-1}[\phi(a)] \implies$

$a+H \subseteq \phi^{-1}[\phi(a)].$

$\forall x \in \phi^{-1}[\phi(a)], \phi(x) = \phi(a) \implies \phi(x-a) = 0' \implies x-a \in H \implies$

$x \in a+H.$

■

Theorem 3. *A ring homomorphism* $\phi : R \mapsto R'$ *is a one-to-one map if and only if* $ker(\phi) = \{0\}$

Proof. Let $H = ker(\phi)$.

$(\longleftarrow)$

$H = \{0\} \implies \forall r \in R, \phi^{-1}[\phi(r)] = \{r+0 = r\} \implies (\phi(x) = \phi(r) \implies x = r)$. OPID.

$(\longrightarrow)$

Let ker(ϕ)$\neq \{0\}$.

since $0 \in$ ker(ϕ), there exists $x \neq 0$, such $x \in$ ker(ϕ).

$\phi(0) = 0' = \phi(x)$, where $0 \neq x$, CaC. OPID.

■

Definition 1. *Let N be a subgroup of a ring R. If* $\forall r \in R, rN \subseteq N$ *and* $Nr \subseteq N$, *we call N an ideal.*

Theorem 4. *N is also a subring.*

Proof. Since N is already a subgroup, we only have to consider if N is closed under multiplication.

$\forall n_1, n_2 \in N, n_1n_2 \in n_1N \subseteq N \implies n_1n_2 \in N$. OPID. ■

Theorem 5. *Let* R/N *be the set of all the additive cosets of N.*

Let $(a+N)+(b+N)$ *be defined as* $(a+b)+N$ *and* $(a+N)(b+N) = ab+N$.

The operation is well defined, and it form a quotient ring R/N, *where* N *is the identity.*

Proof. We prove even if the expression of cosets are different, when put into the operation, we will still have the same result.

Let $c, d \in R$, where $c + N = a + N, d + N = b + N, c \neq a, d \neq b$.

$\forall n_1 \in N, c+n_1 \in a+N \implies c+n_1 = a+n_2, \exists n_2 \in N \implies c = a+n_2-n_1$.

$\forall n_3 \in N, d+n_3 \in b+N \implies d+n_3 = b+n_4, \exists n_4 \in N \implies d = b+n_4-n_3$.

$\forall (c+d)+n_5 \in (c+d)+N, (c+d)+n_5 = (a+b)+(n_5+n_2-n_1+n_4-n_3) \in (a+b)+N \implies (c+d)+N \subseteq (a+b)+N$.

$\forall (a+b)+n_6 \in (a+b)+N, (a+b)+n_6 = (c+d)+(n_1-n_2+n_3-n_4+n_6) \in (c+d)+N \implies (a+b)+N \subseteq (c+d)+N$.

$(a+b)+N = (c+d)+N$. OPID.

Let $c, d \in R$, where $a + N = c + N, b + N = d + N$.

$c = a + n_1, \exists n_1 \in N, d = b + n_2, \exists n_2 \in N$.

$cd = (a + n_1)(b + n_2) = ab + n_1 b + a n_2 + n_1 n_2$.

By premise, $n_1 b + a n_2 + n_1 n_2 \in N$, which give us $cd = ab + n_3, \exists n_3 \in N$.

$\forall cd+n_4 \in cd+N, cd+n_4 = ab+(n_3+n_4) \in ab+N \implies cd+N \subseteq ab+N$.

$\forall ab+n_5 \in ab+N, ab+n_5 = cd+(-n_3+n_5) \in cd+N \implies ab+N \subseteq cd+N$.

$(c+N)(d+N) = cd+N = ab+N$. OPID.

$\forall a+N, b+N \in R/N, (a+N)+(b+N) = (a+b)+N \in R/N$. R/N is closed under addition.

$\forall a+N \in R/N, (a+N)+N = (a+N)+(0+N) = a+N \implies N \in R/N$ is the identity.

$\forall a+N \in R/N, \exists (-a)+N, (a+N)+((-a)+N) = (0+N) = N$. Inverse included. R/N is at least a group.

$\forall a+N, b+N \in R/N, (a+N)+(b+N) = (a+b)+N = (b+a)+N = (b+N)+(a+N)$. R/N is abelian

$\forall a+N, b+N, c+N \in R/N, [(a+N)(b+N)](c+N) = (ab+N)(c+N) = abc+N = (a+N)(bc+N) = (a+N)[(b+N)(c+N)]$. multiplication of R/N is associative.

$\forall a+N, b+N, c+N \in R/N, [(a+N)+(b+N)](c+N) = (a+b+N)(c+N) = (ac+bc)+N = (ac+N)+(bc+N) = (a+N)(c+N)+(b+N)(c+N)$.

$\forall a+N, b+N, c+N \in R/N, (c+N)[(a+N)+(b+N)] = (c+N)(a+b+N) = (ca+cb)+N = (ca+N)+(cb+N) = (c+N)(a+N)+(c+N)(b+N)$. R/N is distributive. In summary, R/N is indeed a ring. ∎

Theorem 6. *Let $\phi : R \mapsto R'$ be a ring homomorphism with kernel H. The operation on the factor ring R/H, $(a+H)+(b+H) = (a+b)+H$, $(a+H)(b+H) = ab+H$ is well defined. Let the map $\mu : R/H \mapsto \phi[R]$ be defined by $\mu(a+H) = \phi(a)$. μ is an isomorphism.*

Proof. We claim H is also an ideal. Then by **Theorem 0.5**, our proof is immediately done.

$\forall a, b \in H, \phi(a+b) = \phi(a)+\phi(b) = 0' \implies a+b \in H$.

$\forall a, b \ni H, \phi(ab) = \phi(a)\phi(b) = 0 \implies ab \in H$. H is closed under both operation.

$\phi(0) = 0'$ by **Theorem 0.1**, which implies $0 \in H$.

$\forall h \in H, \phi(-h) = -\phi(h) = -0' = 0' \implies -h \in H$. Additive inverse included, H is at least a subring.

$\forall a \in R, \forall ah \in aH, \phi(ah) = \phi(a)\phi(h) = 0' \implies ah \in H \implies aH \subseteq H$.

$\forall b \in R, \forall hb \in Hb, \phi(hb) = \phi(h)\phi(b) = 0' \implies hb \in H \implies Hb \subseteq H$.

H is an ideal. OCIP.

$\mu(a+H)+\mu(b+H) = \phi(a)+\phi(b) = \phi(a+b) = \mu((a+b)+H) = \mu((a+H)+(b+H))$.

$\mu(a+H)\mu(b+H) = \psi(a)\psi(b) = \psi(ab) = \mu(ab+H) = \mu((a+H)(b+H))$. μ is a homomorphism.

$\mu(a+H) = \mu(b+H) \implies \phi(a) = \phi(b) \implies \phi(a)-\phi(b) = 0' \implies \phi(a-b) = 0' \implies a-b \in H \implies a = b+h_1, \exists h_1 \in H$.

$\forall a+h_2 \in a+H, a+h_2 = b+(h_1+h_2) \in b+H \implies a+H \subseteq b+H$.

$\forall b+h_3 \in b+H, b+h_3 = a+(-h_1+h_3) \in a+H \implies a+H \subseteq b+H$.

$a+H = b+H$. μ is one-to-one.

$\forall \phi(a) \in \phi[R], \exists a+H \in R/H, \mu(a+H) = \phi(a)$, μ is onto. OPID. ∎

Theorem 7. *Let H be a subring of the ring R. Multiplication of the additive cosets of H is well defined by the equation*

$$(a+H)(b+H) = (ab+H) \tag{1}$$

if and only if $ah \in H$ and $hb \in H$ for all $a, b \in R, h \in H$

Proof. $(\longleftarrow)$

$\forall a, b \in R, \forall h \in H, ah, hb \in H \implies aH \subseteq H, Hb \subseteq H.$

So H is an ideal, then by **Theorem 5**, OPID.

$(\longrightarrow)$

Let there exists a,b,h_1, such $ah_1 \notin H$ or $h_1 b \notin H$.

WOLG, let $h_1 b \notin H$.

Let $c = a + h_1$.

$c + H = a + H$, clearly.

We claim $(c+H)(b+H) = cb + H \neq ab + H$, then CaC.

$cb = (a + h_1)b = ab + h_1 b.$

$cb + H = ab + h_1 b + H.$

$ab + h_1 b + 0 \in cb + H, ab + h_1 b \notin ab + H$, since $h_1 b \notin H$.

This implies $(c+H)(b+H) = cb + H \neq ab + H = (a+H)(b+H)$, even though $(c+H) = (a+H)$.

∎

Theorem 8. *Let N be an ideal of a ring R. then $\gamma : R \to R/N$ given by $\gamma(x) = x + N$ is a ring homomorphism with kernel N.*

Proof. $\forall x, y \in R, \gamma(x) + \gamma(y) = (x+N) + (y+N) = (x+y) + N = \gamma(x+y).$

$\forall x, y \in R, \gamma(x)\gamma(y) = (x+N)(y+N) = xy + N = \gamma(xy).$ γ is a ring homomorphsim.

N is the identity in R/N by **Theorem 5**

$\gamma(x) = N \implies x + N = N \implies \forall n_1, x + n_1 \in N \implies x + n_1 = n_2, \exists n_2 \in N \implies x = n_2 - n_1 \in N \implies ker(\gamma) \subseteq N.$

$\forall n_1 \in N, \gamma(n_1) = n_1 + N = N \implies N \subseteq ker(\gamma)$.

$ker(\gamma) = N$. OPID. ■

Theorem 9. *Let $\phi : R \to R'$ be a ring homomorphism with kernel N. Then the map $\mu : R/N \to \phi[R]$ given by $\mu(x+N) = \phi(x)$ is an isomorphism. If $\gamma : R \to R/N$ is the homomorphism given by $\gamma(x) = x + N$, then for each $x \in R$, we have $\phi(x) = \mu(\gamma(x))$*

Proof. $\mu(x + N) + \mu(y + N) = \phi(x) + \phi(y) = \phi(x + y) = \mu(x + y + N)$.

$\mu(x + N)\mu(y + N) = \phi(x)\phi(y) = \phi(xy) = \mu(xy + N)$.$\mu$ is a ring homomorphism.

$\mu(x + N) = \mu(y + N) \implies \phi(x) = \phi(y) \implies \phi(x - y) = 0 \implies x - y \in N \implies x = y + n_1, \exists n_1 \in N$.

$\forall x + n_2 \in x + N, x + n_2 = y + n_1 + n_2 \in y + N \implies x + N \subseteq y + N$.

$\forall y + n_3 \in y + N, y + n_3 = x - n_1 + n_3 \in x + N \implies y + N \subseteq x + N \implies x + N = y + N$. μ is one-to-one.

$\forall \phi(x) \in \phi[R], \exists x + N \in R/N, \mu(x + N) = \phi(x)$, μ is one-to-one. OPID.

$\forall x \in R, \mu(\gamma(x)) = \mu(x + N) = \phi(x)$. OPID. ■

Example Noted: $GL(n, R)$ is a subring of $M(n, R)$, yet there exists $A \in M(n, R)$ such $det(A) = 0$, $\forall B \in A(GL(n, R)), det(B) = 0 \implies B \notin GL(n, R) \implies A(GL(n, R)) \nsubseteq GL(n, R) \implies$ GL(n,R) is a subring but is not an ideal.

Theory Exercise

17.

Proof. $\forall a+b\sqrt{2}, c+d\sqrt{2} \in R, (a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2} \in R$. R is closed under addition.

$0 = 0 + 0\sqrt{2} =\in R$. Identity included.

$\forall a + b\sqrt{2} \in R, \exists(-a) + (-b)\sqrt{2}, (a + b\sqrt{2}) + [(-a) + (-b)\sqrt{2}] = 0$. Inverse included. R is at least a subgroup.

$\forall a + b\sqrt{2}, c + d\sqrt{2}, (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2} \in R$. R is a subgring.

$\forall \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}, \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \in R', \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & 2(b+d) \\ b+d & a+c \end{bmatrix} \in R'$. R' is closed under addition.

Let $a = 0, b = 0$.

$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \in R'$. Identity included in R'.
$\forall \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \in R', \exists \begin{bmatrix} -a & -2b \\ -b & -a \end{bmatrix} \in R', \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} -a & -2b \\ -b & -a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Inverse included R' is at least a subgroup.

$\forall \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}, \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \in R', \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} ac+2bd & 2ad+2bc \\ bc+ad & ac+2bd \end{bmatrix} \in R'$. R' is a subring.

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

$\phi(a+b\sqrt{2})\phi(c+d\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} ac+2bd & 2ad+2bc \\ bc+ad & ac+2bd \end{bmatrix} = \phi((ac+2bd)+(bc+ad)\sqrt{2}) = \phi((a+b\sqrt{2})(c+d\sqrt{2}))$. ϕ is at least a homomorphism.

$\phi(a+b\sqrt{2}) = \phi(c+d\sqrt{2}) \implies \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} = \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \implies a = c, b = d \implies a+b\sqrt{2} = c+d\sqrt{2}$. ϕ is one-to-one.

$\forall \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \in R', \exists a+b\sqrt{2} \in R, \phi(a+b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$. ϕ is onto.

ϕ is an isomorphism. OPID.

■

18.

Proof. Let F be a field and R be a ring.

Let $\phi : F \to R$ be a ring homomorphism, defined by $\phi(a) = 0', \forall a \in F$.

This definition is obviously well defined.

Now we let $\gamma \neq \phi$ be a ring homomorphism.

Assume there exists $a \neq 0 \in F$, such $\gamma(a) = 0'$.

$\forall b \in F, \gamma(b) = \gamma(baa^{-1}) = \gamma(b)\gamma(a)\gamma(a^{-1}) = 0' \implies \gamma = \phi$, CaC.

So, ker(γ)=$\{0\}$.

$\gamma(a) = \gamma(b) \implies \gamma(a) - \gamma(b) = 0' \implies \gamma(a-b) = 0' \implies a - b = 0 \implies a = b$. γ is one-to-one.

■

19.

Proof. $\forall a, b \in R, \psi\phi(a) + \psi\phi(b) = \psi(\phi(a) + \phi(b)) = \psi\phi(a+b)$.

$\forall a, b \in R, \psi\phi(a)\psi\phi(b) = \psi(\phi(a)\phi(b)) = \psi\phi(ab)$.

■

20.

Proof. $\forall a, b \in R, \phi_p(a+b) = a^p + \sum_{i=1}^{p-1} \binom{p}{i} \cdot a^{p-i}b^i + b^p$.

$\forall i \in [1, p-1], p|\binom{p}{i}$, since p is a prime.

$\implies \sum_{i=1}^{p-1} \binom{p}{i} \cdot a^{p-i}b^i = 0$, since the characteristic value is p.

$\implies \phi_p(a+b) = a^p + b^p = \phi_p(a) + \phi_p(b)$.

$\forall a, b \in R, \phi_p(a)\phi_p(b) = a^p b^p = (ab)^p = \phi_p(ab)$, since R is a commutative ring.

■

21.

Proof. $\forall a \in R', \exists b \in R, b \notin ker(\phi), (a\phi(1))\phi(b) = a(\phi(1)\phi(b)) = a\phi(b) \implies (a\phi(1) - a)\phi(b) = 0'$.

Since R' have no zero-divisor, and $\phi(b) \neq 0'$, $a\phi(1) - a = 0' \implies a\phi(1) = a$.

■

22.

(a)

Proof. $\forall \phi(a) \in \phi[R], \forall \phi(n) \in \phi[N], \phi(a)\phi(n) = \phi(an)$, where $an \in N$, which implies $\phi(an) \in \phi(N) \implies \phi(a)\phi[N] \subseteq \phi[N]$.

$\forall \phi(a) \in \phi[R], \forall \phi(n) \in \phi[N], \phi(n)\phi(a) = \phi(na)$, where $na \in N$, which implies $\phi(na) \in \phi(N) \implies \phi[N]\phi(a) \subseteq \phi[N]$.

■

(b)

Proof. Let R be $\mathbb{Z}[x]$, and N be the set of all polynomials in which every coefficient c satisfy the property $c = 2n, \exists n \in \mathbb{Z}$.

N is additive closed under since $\forall c_1, c_2, c_1 + c_2 = 2(n_1 + n_2), \exists n_1, n_2 \in \mathbb{Z}$.

$0 \in N$, clearly.

Inverse exists since $\forall f \in N$, the coefficients of $-f$ are just $-c$ where c are the coefficients of f.

N is at least a subgroup.

N is an ideal, since every integer-coefficient polynomial times even-integer-coefficient polynomial is still even-integer-coefficient polynomial.

Let R' be $Q[x]$.

Let $\phi : R \to R'$ be defined by $\phi(f) = f$.

$2 \in \phi[N], \frac{3}{2} \in R'$.

$(\frac{3}{2})2 = 3 \notin \phi[N] \implies (\frac{3}{2})\phi[N] \nsubseteq \phi[N]$.

■

(c)

Proof. Arbitrarily pick $a \in R$ and $n \in \phi^{-1}[N']$.

$\phi(an) = \phi(a)\phi(n)$, where $\phi(n) \in N'$, which implies $\phi(an) = \phi(a)\phi(n) \in N' \implies an \in \phi^{-1}[N']$.

This shows $\forall a, a\phi^{-1}[N'] \subseteq \phi^{-1}[N']$.

Arbitrarily pick $a \in R$ and $n \in \phi^{-1}[N']$.

$\phi(na) = \phi(n)\phi(a)$, where $\phi(n) \in N'$, which implies $\phi(na) = \phi(n)\phi(a) \in N' \implies na \in \phi^{-1}[N']$.

This shows $\forall a, \phi^{-1}[N']a \subseteq \phi^{-1}[N']$. OPID.

■

23.

Proof. Arbitrarily pick $g \in F[x_1, \cdots, x_n]$ and $f \in N_S$.

$\forall(a_1, \cdots, a_n), (gf)(a_1, \cdots, a_n) = g(a_1, \cdots, a_n)f(a_1, \cdots, a_n) = g(a_1, \cdots, a_n)0 = 0 \implies gf \in N_S \implies N_S$ is at least a left ideal.

$\forall(a_1, \cdots, a_n), (fg)(a_1, \cdots, a_n) = f(a_1, \cdots, a_n)g(a_1, \cdots, a_n) = 0g(a_1, \cdots, a_n) = 0 \implies fg \in N_S \implies N_S$ is an ideal.

■

24.

Proof. Let N be an ideal of a field F.

We consider two situation, one is $1 \in N$, another is $1 \notin N$.

Case: $1 \in N$

$\forall a \in F \setminus N, a \in aN$, yet $a \notin N \implies aN \nsubseteq N$.

This give us $F \setminus N = \varnothing \implies N = F \implies F \setminus N = \{N\}$. OPID.

Case: $1 \notin N$

Assume there exists $a \neq 0 \in N$.

$1 \in a^{-1}N$, yet $1 \notin N \implies a^{-1}N \nsubseteq N$, CaC.

So, $N = \{0\}$.

Let $\phi : F \to F/N$ be defined by $\phi(x) = x + N$.

ϕ is clearly a homomorphism by **theorem 0.8**.

$\phi(a) = \phi(b) \implies a + N = b + N \implies \{a\} = \{b\} \implies a = b$. ϕ is one-to-one.

ϕ is clearly onto.

$F \simeq F/N$. OPID.

■

25.

Proof. Let 1 be the unity of R.

We claim $1 + N$ is the unity of R/N.

$\forall r + N \in R/N, (1+N)(r+N) = (r+N), (r+N)(1+N) = (r+N)$. OPID.

■

26.

Proof. $\forall r \in R, x \in I_a, a(rx) = (ax)r = 0r = 0 \implies rx \in I_a \implies I_a$ is at least a left ideal.

$\forall r \in R, x \in I_a, a(xr) = (ax)r = 0r = 0 \implies xr \in I_a \implies I_a$ is an ideal.

■

27.

Proof. Let N_1, N_2 be two ideals of a ring R.

$\forall a, b \in N_1 \cap N_2, a + b \in N_1, a + b \in N_2 \implies a + b \in N_1 \cap N_2$. $N_1 \cap N_2$ is closed under addition.

$0 \in N_1, 0 \in N_2 \implies 0 \in N_1 \cap N_2$.

$\forall a \in N_1 \cap N_2, -a \in N_1, -a \in N_2 \implies -a \in N_1 \cap N_2$. $N_1 \cap N_2$ is at least a subgroup.

$\forall r \in R, \forall n \in N_1 \cap N_2, rn \in N_1$, since N_1 is an ideal.

$rn \in N_2$, since N_2 is an ideal.

$\implies rn \in N_1 \cap N_2 \implies N_1 \cap N_2$ is at least a left ideal.

$\forall r \in R, \forall n \in N_1 \cap N_2, nr \in N_1$, since N_1 is an ideal.

$nr \in N_2$, since N_2 is an ideal.

$\implies rn \in N_1 \cap N_2 \implies N_1 \cap N_2$ is an ideal.

■

28.

Proof. Let $\phi_* : R/N \to R'/N'$ be defined by $\phi_*(N + a) = N' + \phi(a)$.

We prove this definition make ϕ_* a ring homomorphism.

$\forall N+a, N+b \in R/N, \phi_*(N+a)+\phi_*(N+b) = (N'+\phi(a))+(N'+\phi(b)) = N' + (\phi(a) + \phi(b)) = N' + (\phi(a + b)) = \phi_*(N + (a + b)) = \phi_*((N + a) + (N + b))$. ϕ_* is at least a group homomorphism.

$\forall N+a, N+b \in R/N, \phi_*(N+a)\phi_*(N+b) = (N'+\phi(a))(N'+\phi(b)) = N'+\phi(a)\phi(b) = N'+\phi(ab) = \phi_*(N+ab) = \phi_*((N+a)(N+b))$. OPID. ■

29.

Proof. We first have to prove R' have a unity.

We claim $\phi(1)$ is the unity in R', where 1 is the unity in R. (1)

$\forall r' \in R', r'\phi(1)\phi(u) = r'\phi(u) \implies (r'\phi(1) - r')\phi(u) = 0'$. (4)

We claim $\phi(u) \neq 0'$.

Assume $\phi(u) = 0'$. (2)

$\phi(u^{-1})\phi(u) = \phi(1) \implies \phi(1) = 0'$.

Then $\forall r \in R, \phi(r) = \phi(r)\phi(1) = 0'$. ϕ will be a null homomorphism, and it clearly can not be onto a nonzero ring R'. So, CaC. OCIP. (2)

We claim $\phi(u)$ is not a zero divisor. (3)

WOLG, assume there exists $c' \neq 0' \in R'$, such $c'\phi(u) = 0'$.

Since ϕ is onto. $\exists c \in R$, such $\phi(c) = c'$.

$0' = (c'\phi(u))\phi(u^{-1}) = c'(\phi(u)\phi(u^{-1})) = c'\phi(1) = \phi(c)\phi(1) = \phi(c) = c' \neq 0'$, CaC. OCIP. (3)

So, $\phi(u)$ is neither $0'$ or a zero divisor in R'. Then , back to statement (4), this give use $r'\phi(1) - r' = 0'$.

$r'\phi(1) - r' = 0' \implies r'\phi(1) = r'$. OCIP. (1)

$\phi(u)\phi(u^{-1}) = \phi(1)$. OPID. ■

30.

Proof. Let H be all the nilpotent elements in a commutative ring R.

Let $a, b \in H$, where $a^{n_1} = b^{n_2} = 0, \exists n_1, n_2 \in \mathbb{N}$.

$(a+b)^{n_1+n_2} = \sum_{i=0}^{n_1+n_2} \binom{n_1+n_2}{i} a^i b^{n_1+n_2-i}$.

If $i > n_1, a^i = 0 \implies \binom{n_1+n_2}{i} a^i b^{n_1+n_2-i} = 0$.

If $i \leq n_1, n_1 + n_2 - i \geq n_2 \implies b^{n_1+n_2-i} = 0 \implies \binom{n_1+n_2}{i} a^i b^{n_1+n_2-i} = 0.$

This give us $(a+b)^{n_1+n_2} = \sum_{i=0}^{n_1+n_2} \binom{n_1+n_2}{i} a^i b^{n_1+n_2-i} = \sum_{i=0}^{n_1+n_2} 0 = 0.$

H is closed under addition.

$0^1 = 0 \implies 0 \in H.$

Let $a \in H$, where $a^{n_1} = 0, \exists n_1 \in \mathbb{N}.$

We claim $(-a)^{n_1} = 0.$

We prove our claim by induction.

Base step: When $n = 1$, $(-a)^n = a^n$ or $-a^n$.

$(-a)^1 = -a^1.$

Induction step: Given when $n = k$, $(-a)^n = a^n$ or $-a^n$. Prove when $n = k + 1$, $(-a)^n = a^n$ or $-a^n$.

$(-a)^{k+1} = (-a)^k(-a) = a^k(-a)$ or $(-a^k)(-a)$.

$a^k(-a) + a^{k+1} = a^k(-a + a) = 0 \implies a^k(-a) = -a^{k+1}.$

$(-a^k)(-a) + (-a^{k+1}) = (-a^k)(-a) + [-((a^k)a)] = (-a^k)(-a) + (-a^k)a = (-a^k)(-a + a) = 0 \implies (-a^k)(-a) = a^k + 1.$

$(-a)^{n_1} = a^{n_1}$ or $-a^{n_1} = 0$ or 0. OCIP.

H is at least a subgroup.

Arbitrarily pick $r \in R, a \in H$. We know $a^n = 0, \exists n \in \mathbb{N}.$

$(ar)^n = (ra)^n = r^n a^n = 0$, since R is commutative.

This give us $ra \in H, ar \in H.$

So H is indeed an ideal.

■

31.

Proof. The nilradical of $\mathbb{Z}_{12}$ is $\{0, 6\}$.

The nilradical of $\mathbb{Z}$ is $\{0\}$.

The nilradical of $\mathbb{Z}_{32}$ is $\{n \in \mathbb{Z}_{32} | \ 2|n\}$ ■

32.

Proof. Let $a + N \in R/N$ be nilpotent.

Then $\exists n \in \mathbb{N}, a^n + N = (a + N)^n = N$. where N is the additive identity in R/N.

$a^n + N = N \implies a^n \in N$.

So a^n is nilpotent, then $\exists n_1 \in \mathbb{N}, (a^n)^{n_1} = 0 \implies a^{nn_1} = 0 \implies a$ is nilpotent $\implies a \in N \implies a + N = N$.

Since $a + N$ is arbitrarily picked, every cosets that is nilpotent is N, which tell us that the nilradical of R/N is $\{N\}$.

■

33.

Proof. Since the nilradical of R/N is R/N, $\forall a \in R, \exists n \in \mathbb{N}, a^n + N = (a + N)^n = N \implies a^n \in N$.

Since every element in N is nilpotent, a^n is nilpotent $\implies \exists n_1 \in \mathbb{N}, a^{nn_1} = (a^n)^{n_1} = 0 \implies a$ is nilpotent, where a is arbitrarily picked from R. This tells us taht every element in R is nilpotent, so the nilradical of R is R itself.

■

34.

Proof. Let $a, b \in \sqrt{N}$, where $\exists n_1, n_2 \in \mathbb{N}, a^{n_1}, b^{n_2} \in N$.

$(a + b)^{n_1+n_2} = \sum_{i=0}^{n_1+n_2} \binom{n_1+n_2}{i} a^i b^{n_1+n_2-i}$.

If $i \geq n_1$, $a^i = a^{n_1}a^{i-n_1} \in N \implies \binom{n_1+n_2}{i} a^i b^{n_1+n_2-i} \in N$.

If $0 \geq i < n_1$, $b^{n_1+n_2-i} = b^{n_2}b^{n_1-i} \in N \implies \binom{n_1+n_2}{i} a^i b^{n_1+n_2-i} \in N$.

So $\forall 0 \leq i \leq n_1 + n_2$, $\binom{n_1+n_2}{i} a^i b^{n_1+n_2-i} \in N \implies (a + b)^{n_1+n_2} = \sum_{i=0}^{n_1+n_2} \binom{n_1+n_2}{i} a^i b^{n_1+n_2-i} \in N \implies a + b \in \sqrt{N}$. $\sqrt{N}$ is closed under addition.

$0^1 = 0 \in N \implies 0 \in \sqrt{N}$.

Let $a \in \sqrt{N}$, where $\exists n \in \mathbb{N}, a^n \in N$.

$(-a)^n = a^n$ or $(-a^n) \in N \implies -a \in \sqrt{N}$. $\sqrt{N}$ is at least a subgroup.

Let $a \in \sqrt{N}$, where $\exists n \in \mathbb{N}, a^n \in N$.

$\forall r \in R, (ra)^n = (ar)^n = r^n a^n \in N$, since R is commutative and N is an ideal.

Since a is arbitrarily picked from $\sqrt{N}$, and r is arbitrarily picked from R, $\sqrt{N}$ is an ideal. OPID.

■

35.

(a)

Proof. Let $R = \mathbb{Z}_0^+$, and let N be $4\mathbb{Z}_0^+$.

$\sqrt{N} = 2\mathbb{Z}_0^+ \neq N$.

■

(b)

Proof. Let $R = \mathbb{Z}_0^+$, and let N be $2\mathbb{Z}_0^+$.

$\sqrt{N} = N$ ■

(c)

Proof. Let H be the nilradical of R/N.

$\forall \sqrt{n} \in \sqrt{N}, \exists m \in \mathbb{N}, (\sqrt{n})^m \in N \implies (\sqrt{n} + N)^m = N \implies \sqrt{n} + N \in H \implies \sqrt{n} \in \bigcup H \implies \sqrt{N} \subseteq \bigcup H$.

Let S be a nilpotent coset of N, $\forall a \in S, a + N = S$.

Since $a + N = S$ is nilpotent, $\exists m \in \mathbb{N}, a^m + N = (a + N)^m = N \implies a^m = N \implies a \in \sqrt{N}$.
Since S can be arbitrarily picked from H, and a can be arbitrarily picked from S.

$\forall a \in \bigcup H, a \in \sqrt{N} \implies \bigcup H \subseteq \sqrt{N}$.

So, $\bigcup H = \sqrt{N}$.

■

37.

Proof. $\phi(a + bi) + \phi(c + di) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} a + c & b + d \\ -(b + d) & a + c \end{bmatrix} = \phi((a + c) + (b + d)i) = \phi((a + bi) + (c + di))$.

$\phi(a+bi)\phi(c+di) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{bmatrix} = \phi(ac - bd + (ad+bc)i) = \phi((a+bi)(c+di))$. ϕ is at least a homomorphism.

$\phi : \mathbb{C} \to \phi[\mathbb{C}]$ is obviously onto.

$\phi(a+bi) = \phi(c+di) \implies \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \implies a = c, b = d \implies a + bi = c + di$. ϕ is an isomorphism.

$\forall \phi(a+bi), \phi(c+di) \in \phi[\mathbb{C}], \phi(a+bi) + \phi(c+di) = \phi(a+c+(b+d)i) \in \phi[\mathbb{C}], \phi(a+bi)\phi(c+di) = \phi(ac-bd+(bc+ad)i) \in \phi[\mathbb{C}]$. $\phi[\mathbb{C}]$ is at least closed under addition and multiplication.

$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \phi(0) \in \phi[\mathbb{C}]$.

$\forall \phi(a+bi) \in \phi[\mathbb{C}], \phi(-a-bi) + \phi(a+bi) = \phi(0) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Inverse included.

$\phi[C]$ is a subring.

■

38.

(a)

Proof. $\forall x, y \in R, \lambda_a(x) + \lambda_a(y) = ax + ay = a(x+y) = \lambda_a(x+y)$.

■

(b)

Proof. $\forall \lambda_a, \lambda_b \in R', \forall r \in R, \lambda_a(r) + \lambda_b(r) = ar + br = (a+b)r = \lambda_{a+b}(r)$, where $\lambda_{a+b} \in R'$. R' is at least closed under addition.

$\forall \lambda_a, \lambda_b \in R', \forall r \in R, \lambda_a(\lambda_b(r)) = \lambda_a(br) = abr = \lambda_{ab}(r)$, where $\lambda_{ab} \in R'$. R' is at least closed under addition and multiplication.

$\forall \phi \in End(\langle R, + \rangle), \forall r \in R, (\lambda_0 + \phi)(r) = 0r + \phi(r) = \phi(r)$. $\lambda_0 \in R'$ is the identity.

$\forall \lambda_a \in R', \forall r \in R, (\lambda_{-a} + \lambda_a)(r) = -ar + ar = 0 = \lambda_0(r)$. Inverse included. R' is a subring.

■

(c)

Proof. let $\phi : R' \to R$ be defined by $\phi(\lambda_a) = a$.

$\phi(\lambda_a) + \phi(\lambda_b) = a + b = \phi(\lambda_{a+b}) = \phi(\lambda_a + \lambda_b)$.

$\phi(\lambda_a)\phi(\lambda_b) = ab = \phi(\lambda_{ab}) = \phi(\lambda_a\lambda_b)$. ϕ is at least a homomorphism.

ϕ is obviously onto.

$\phi(\lambda_a) = \phi(\lambda_b) \implies a = b \implies \lambda_a = \lambda_b$. ϕ is one-to-one. ϕ is an isomorphism.

■