Solutions to Past Preliminary Algebra Exams

Joseph McGuire

August 20, 2020

Spring 2018

1. *Let G be a group and $a \in G$ be an element. Let $n \in \mathbb{N}$ be the smallest positive numbers such that $a^n = e$ is the identity element. Show that the set $\{e, a, a^2, ..., a^{n-1}\}$ contains no repetitions.*

Proof. Assume G is a group and $a \in G$ and that $n \in \mathbb{N}$ is the smallest positive integer such that $a^n = e$, with e the identity element of G. Then for sake of contradiction, suppose that $\{e, a, a^2, ..., a^{n-1}\}$ contains at least one repeated element. That is there exists $m, k \in \{1, ..., n\}$ with $m \neq k$ such that $a^m = a^k$. Without loss of generality, assume that $m > k$. Then $(a^k)^{-1}a^m = e \implies a^{-k}a^m = e \implies a^{m-k} = e$. Note that $m, k \in \{1, ..., n\}$ and $m - k > 0$, so that $m - k \in \{1, ..., n\}$, but that $m - k < n$. So there's an integer less than n such that $a^{m-k} = e$, a contradiction of out hypothesis. Thus the set $\{e, a, ..., a^{n-1}\}$ contains no repeats. $\square$

2. *Let G be a finite group and $H, K \trianglelefteq G$ be normal subgroups of relatively prime order. Prove that G is isomorphic to a subgroup of $G/H \times G/K$.*

Proof. Let G be a finite group with normal subgroups H, K such that $\gcd(|H|, |K|) = 1$. Then consider the mapping from $G \to G/H \times G/K$, given by $\phi(g) : g \mapsto (gH, gK)$. This is a homomorphism since $\phi(g \cdot m) = ((g \cdot m)H, (g \cdot m)K) = (gH, gK) \cdot (mH, mK) = \phi(g)\phi(k)$. Then note that $\ker(\phi) = H \cap K$, however if $x \in H \cap K$, then $|x|$ divides $|H|$ and $|x|$ divides $|K|$. However we know $\gcd(|H|, |K|) = 1$, so that $|x| = 1 \implies x = e$, the identity of G. So that by the properties of homomorphism that ϕ is a $1-1$ function onto it's range: $\{(gH, gK) \in G/H \times G/K : g \in G\}$. Both the kernel and the range are guarenteed to be subgroups of G and $G/H \times G/K$, respectively, because ϕ is a homomorphism. Thus $\{(gH, gK) \in G/H \times G/K : g \in G\} \cong G$ $\square$

3. *Prove that if $\phi : R \to S$ is a surjective ring homomorphism between commutative rings with unity, then $\phi(1_R) = 1_S$.*

Proof. Let $\phi : R \to S$ be a surjective ring homomorphism between commutative rings with unity, R and S. Then for any $y \in S$, there's a $x \in R$ such that $\phi(x) = y$. So that $\phi(1_R \cdot x) = \phi(x)$ and $\phi(1_R \cdot x) = \phi(1_R) \cdot \phi(x)$. Hence, for any $y \in S$, $\phi(x) = \phi(1_R) \cdot \phi(x) \implies y = \phi(1_R)y \implies \phi(1_R) = 1_S$. $\square$

4. *Let $V \subset \mathbb{R}^5$ be the subspace defined by the equation*

$$x_1 - 2x_2 + 3x_3 - 4x_4 + 5x_5 = 0$$

4.1. *Find with justification a basis of V.*

Solution. *First, note that we can write the defining equation of this subspace as: $x_1 = 2x_2 - 3x_3 + 4x_4 - 5x_5$. So then any vector in this subspace is given by:*

$$\begin{aligned}(2x_2 - 3x_3 + 4x_4 - 5x_5, x_2, x_3, x_4, x_5) &= x_2(2,1,0,0,0) + x_3(-3,0,1,0,0) + x_4(4,0,0,1,0) + x_5(-5,0,0,0,1) \\ &= span((2,1,0,0,0), (-3,0,1,0,0), (4,0,0,1,0), (-5,0,0,0,1)).\end{aligned}$$

We'll show that this is a spanning and linearlly independent list of vectors: $(2,1,0,0,0), (-3,0,1,0,0), (4,0,0,1,0), (-5,0,0$ *If v is in this subspace then x_1 must satisfy the defining equation. Hence any element in this subspace must be in the span of our list. For linearally independence we set $a(2,1,0,0,0) + b(-3,0,1,0,0) + c(4,0,0,1,0) + d(-5,0,0,0,1) = (0,0,0,0,0)$. This implies $a = b = c = d = 0$. Hence this list is linearally independent and spanning of the subspace and so is a basis of it.*

4.2. *Find with justification a basis for $V^\perp$, the subspace of $\mathbb{R}^5$ orthogonal to V under the usual dot product.*

Solution. *Note that span(...)$^\perp$ = ...$^\perp$ for any list .... So that we'll find the orthogonal complement of our list:* $(2,1,0,0,0)\cdot(a,b,c,d,e)=0 \implies 2a+b=0$, $(-3,0,1,0,0)\cdot(a,b,c,d,e)=0 \implies -3a+c=0$, $(4,0,0,1,0)\cdot(a,b,c,d,e)=0 \implies 4a+d=-$, $(-5,0,0,0,1)\cdot(a,b,c,d,e)=0 \implies -5a+e=0$. *This gives us the vector* $(1,-2,3,-4,5) \implies V^\perp = span(1,-2,3,-4,5)$

5. *Suppose that V is a finite-dimensional real vector space and $T : V \to V$ is a linear transformation. Prove that T has at most* $\dim(range(T))$ *distinct nonzero eigenvalues.*

Proof. Let V be a finite-dimensional real vector space, with dimension n, and $T : V \to V$ is a linear transformation. Suppose, for sake of contradiction, that there are at least $n+1$ distinct non-zero eigenvalues of T. Then there must be at least $n+1$ associated non-zero eigenvectors of T. Additionally, these are linearly independent vectors. However, by the Rank-Nullity theorem we have $n = \dim(\text{null}(T)) + \dim(\text{range}(T))$. Furthermore, eigenvalues are by definition in the range of T. So we have $\dim(\text{range}(T)) \geq n+1$, a contradiction of the Rank-Nullity theorem. Thus there must be at most $\dim(\text{range}(T))$ many distinct non-zero eigenvalues. □

Spring 2017

6. *Let $V = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} : a_0, a_1, a_2 \in \mathbb{Q}\} \subseteq \mathbb{R}$. This set is a vector space over $\mathbb{Q}$*

6.1. *Verify V is closed under product (using the usual product operation in $\mathbb{R}$).*

Solution. *Let $x = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}$ and $y = b_0 + b_1\sqrt[3]{2} + b_2\sqrt[3]{4}$, for $a_0, a_1, a_2, b_0, b_1, b_2 \in \mathbb{Q}$. And note that $\sqrt[3]{4} = (\sqrt[3]{2})^2$ Then $xy = (a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4})(b_0 + b_1\sqrt[3]{2} + b_2\sqrt[3]{2}) = a_0b_0 + a_0b_12^{1/3} + a_0b_24^{1/3} + a_1b_02^{1/3} + a_1b_14^{1/3} + a_1b_2 + a_2b_04^{1/3} + a_2b_12 + a_2b_22(2^{1/3})$. This obtained after a substantial amount of algebra. This has the form of elements of V, hence V is closed under the product operation.*

6.2. *Let $T : V \to V$ be the linear transformation defined by $T(v) = (\sqrt[3]{2} + \sqrt[3]{4})v$. Find the matrix representing T with respect to the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ for V.*

Solution. $T(1) = (\sqrt[3]{2} + \sqrt[3]{4}) = 0 + \sqrt[3]{2} + \sqrt[3]{4}$. $T(\sqrt[3]{2}) = 4 + 0\cdot\sqrt[3]{2} + \sqrt[3]{4}$. $T(\sqrt[3]{4}) = 2 + 2(2^{1/3}) + 0\cdot(4^{1/3})$. *This will correspond to the matrix:*

$$\begin{bmatrix} 0 & 2 & 2 \\ 1 & 0 & 2 \\ 1 & 1 & 0 \end{bmatrix}$$

6.3. *Determine the characteristic polynomial for T.*

Solution. *Taking the determinant of the matrix $T - \lambda I_3$:*

$$\begin{aligned} \det(T - \lambda I_3) &= -\lambda(\lambda^2 - 2) - 1(-2\lambda - 2) + 1(4 + 2\lambda) \\ &= -\lambda^3 + 2\lambda + 2\lambda + 2 + 4 + 2\lambda \\ &= -\lambda^3 + 6\lambda + 6. \end{aligned}$$

This is the characteristic polynomial of the matrix representation of T with the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

7. *Suppose F is a field and A is a $n \times n$ matrix over F. Suppose further that A posses distinct eigenvalues λ_1, λ_2 with* $\dim(\text{Null}(A - \lambda_1 I_n)) = n - 1$. *Prove A is diagonalizable.*

Proof. Let F be a field and A an $n \times n$ over F. Suppose A has exactly two distinct eigenvalues λ_1, λ_2 with $\dim(\text{Null}(A - \lambda_1 I_n)) = n - 1$. Note that this is the eigenspace of the eigenvalue λ_1. So there are $n-1$ eigenvectors with the eigenvalue λ_1 that are a basis of $\text{Null}(A - \lambda_1 I_n)$. Additionally λ_2 must have at least one eigenvector that is linearly independent from any of the eigenvectors in $\text{Null}(A - \lambda_1 I_n)$. So we have a set of n linearly independent eigenvectors of A, hence this set is a basis of A. We can find a representation of A in terms of this basis, call it, $\{v_2, v_{1,1}, ..., v_{1,n-1}\}$, such that $Av_{1,i} = \lambda_1 v_{1,i}$ for all $i \in \{1, ..., n-1\}$ and $Av_2 = \lambda_2 v_2$. This will give us the matrix representation:

$$\begin{bmatrix} \lambda_2 & 0 & \dots & 0 \\ 0 & \lambda_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_1 \end{bmatrix}$$

Hence A is diagonalizable with eigenvalue entries. $\square$

8.

8.1. *Suppose N is a normal subgroup of a group G and $\pi_N : G \to G/N$ is the usual projection homomorphism, defined by $\pi_N(g) = gN$. Prove that if $\phi : G \to H$ is any homomorphism with $N \leq \ker(\phi)$, then there exists a unique homomorphism $\phi : G/N \to H$ such that $\phi = \psi \circ \pi_N$. (You must explicitly define ϕ, show it's well defined, show $\phi = \psi \circ \pi_N$, and show that ψ is uniquely determined.)*

Proof. Let $\pi_N : G \to G/N$ be given by $\pi_N(g) = gN$ and take $\psi : G \to H$ to be any group homomorphism. Then let $\phi : G/N \to H$ be given by $\phi(gN) = \psi(g)$. So that $\phi(\pi_N(g)) = \phi(gN) = \psi(g)$ for any $g \in G$, so that $\phi \circ \pi_N = \psi$. We'll show that this is a well defined function and is uniquely determined. Let $(gN, y) \in \phi$ and $(gN, z) \in \phi$, then $\phi(gN) = \psi(g) = y$ and $\phi(gN) = \psi(g) = z$, and since ψ is well-defined, we have $y = z$, and thus ϕ is well-defined. Let $\psi = \phi_1 \circ \pi_N$ and $\psi = \phi_2 \circ \pi_N$. Then $\phi_2(\phi_N(g)) = \phi_2(gN) = \psi(g) = \psi_1(gN)$ for all $g \in G$ and hence $\psi_1 = \psi_2$ and ψ is uniquely determined. $\square$

8.2. *Prove:* ***Third Isomorphism Theorem****: If $M, N \trianglelefteq G$ with $N \leq M$, then $(G/N)/(M/N) \cong G/M$.*

Proof. Let M, N be normal subgroups of G and N a subgroup of M. Then consider the homomorphism $\phi : gN \mapsto gM$, for $g \in G$, this is in fact a homomorphism between G/N and G/M, since $phi(gN \cdot hN) = \phi((gh)N) = (gh)M = gM \cdot hM = \phi(gN) \cdot \phi(hN)$. And well-defined: $(gN, gM), (gN, hM) \in \phi \implies \phi(gN) = gM$ and $\phi(gN) = hM \implies gM = hM$. Additionally, this homomorphism has a kernel of M/N and range of G/M. To show this $xN \in \ker(\phi)$, then $\phi(xN) = M$ and hence $x \in M$ and so $xN \in M/N$. Conversely, if $mN \in M/N$, then $\phi(mN) = mM = M$, and thus $\ker(\phi) = M/N$. For the range, take $gM \in G/M$, then this will correspond to $\phi(gN) = gM$, so that $G/M \subseteq \text{range}(\phi)$. Clearly, $\text{range}(\phi) \subseteq G/M$. So that $G/M = \text{range}(\phi)$.

Finally, by the first isomorphism theorem we have that $(G/N)/(M/N) \cong G/M$. $\square$

9. *Explicitly list all group homomorphisms $f : \mathbb{Z}_6 \to \mathbb{Z}_{12}$.*

Solution. *First, note the following: in $(\mathbb{Z}_6, +)$: $|0| = 1, |1| = 6, |2| = 3, |3| = 2, |4| = 3, |5| = 6$ and in $(\mathbb{Z}_{12}, +) : |0| = 1, |1| = 12, |2| = 6, |3| = 4, |4| = 3, |5| = 12, |6| = 2, |7| = 12, |8| = 3, |9| = 4, |10| = 6, |11| = 12$. Additionally any homomorphism must satisfy $|x| = n, \implies |\phi(x)| \big| n$ and that $\ker(\phi)$ must be a subgroup of $\mathbb{Z}_6$. The subgroups of $\mathbb{Z}_6$ are exactly: $\{0\}, \mathbb{Z}_6, 0, 2, 4, \{0, 3\}$. So that for $\mathbb{Z}_6$ this is the null map: $\phi_0 : x \to 0$ for all $x \in \mathbb{Z}_6$. For $\{0\}$, the possibilities are $\phi_1(0) = 0, \phi_1(1) = 2, 10, \phi_1(2) = 2\phi_1(1), \phi_1(3) = 3\phi_1(1), \phi_1(4) = 4\phi_1(1), \phi_1(5) = 5\phi_1(1)$, we can rule out $\phi_1(1) = 10$, since we would have $\phi_1(5) = 0$, so that $\phi_1(1) = 2$. For $\{0, 2, 4\}$, we would have $\phi_2(0) = 0, \phi_2(2) = 0, \phi_2(4) = 0$ with $\phi_2(1) = 2or10, \phi_2(3) = \phi_2(2) + \phi_2(1) = \phi_2(1), \phi_2(5) = \phi_2(4) + \phi_2(1) = \phi_2(1)$, so that there are two homomorphisms here, one where $\phi_2(1) = 2$ and the other $\phi_2(1) = 10$. For $\{0, 3\}$ we have $\phi_3(0) = 0, \phi_3(3) = 0$ and $\phi_3(1) = 2or10, \phi_3(2) = 2\phi_3(1), \phi_3(4) = 4\phi_3(1), \phi_3(5) = \phi_3(3) + \phi_3(2) = 2\phi_3(1)$. So that again we have two homomorphisms with $\phi_3(1) = 2$ and $\phi_3(1) = 10$.*

So in total we have 6 homomorphisms between $(\mathbb{Z}_6, +) \to (\mathbb{Z}_{12}, +)$.

10. *Let $\epsilon : \mathbb{R}[x] \to \mathbb{C}$ be the ring homomorphism that is evaluation at i, so $\epsilon(f) = f(i)$. (Here i denotes the complex number sometimes denoted $\sqrt{-1}$.)*

10.1. *Prove that $\ker(\epsilon) = (x^2 + 1) \subseteq \mathbb{R}[x]$.*

Proof. Consider $f(x) \in \ker(\epsilon)$, then $f(i) = 0$, so that i is a root of f, by the complex conjugate root theorem, $-i$ is also a root of f. So that f can be factored as follows $f(x) = (x - i)(x + i)q(x)$, for $q(x) \in \mathbb{R}[x]$, but this isn't in $\mathbb{R}[x]$. So that $f(x) = (x^2 + 1)q(x) \in (x^2 + 1)$. Hence $\ker(\epsilon) \subseteq (x^2 + 1)$. Conversely $f(x) \in (x^2 + 1)$, then $f(x) = (x^2 + 1)q(x)$ for $q(x) \in \mathbb{R}[x]$. Clearly $f(i) = 0q(x) = 0 \in \ker(\epsilon)$. So that $\ker(\epsilon) = (x^2 + 1) \subseteq \mathbb{R}[x]$. $\square$

10.2. *Prove that $(x^2 + 1)$ is a maximal ideal in $\mathbb{R}[x]$.*

Proof. Let J be an ideal in $\mathbb{R}[x]$ such that $(x^2 + 1) \subseteq J \subseteq \mathbb{R}[x]$. Note any ideal in $\mathbb{R}[x]$ is principal, so that there exists a minimal polynomial such that $(p(x)) = J$. So $(x^2 + 1) \subseteq (p(x)) \subseteq \mathbb{R}[x]$.

So there exists a $q(x) \in \mathbb{R}[x]$ such that $x^2 + 1 = q(x)p(x)$ with $\deg(p(x)) + \deg(q(x)) = 2 \implies \deg(p(x)) \leq 2$. If $\deg(p(x)) = 0$, then $(p(x)) = \mathbb{R}[x]$. If $\deg(p(x)) = 1$, then $p(x) = Ax + B$ for some $A, B \in \mathbb{R}$. So that $(Ax + B)(Cx + D) = x^2 + 1$ and $x^2 + 1$ has at least one real root $x = -\frac{B}{A}$, $A \neq 0$ since $\deg(p(x)) = 1$. This isn't possible since we know the only two roots of $x^2 + 1$ are $-i, i$. Finally, if $\deg(p(x)) = 2$, then $\deg(r(x)) = 0$ and $r(x) = C$ for $C \in \mathbb{R}$. So that $C(Ax^2 + Bx + D) = (x^2 + 1)$. So then we must have $CD = 1$, $AC = 1$ and $CB = 0$, since $\mathbb{R}$ is an integral domain this means $B = 0$ and so we have $p(x) = x^2 + 1$.

Thus any ideal between $(x^2 + 1)$ and $\mathbb{R}[x]$ is either $\mathbb{R}[x]$ or $(x^2 + 1)$, hence $(x^2 + 1)$ is a maximal ideal in $\mathbb{R}[x]$. $\square$

Spring 2016

11. *Without using Cauchy's Theorem or the Sylow Theorem, prove that every group of order* 21 *contains an element of order* 3.

Proof. . First, we'll note that in any group of order n, with $a \in G$ and $k \in \mathbb{N}$, we have that $| < a^k > | = | < a^{\gcd(n,k)} > |$ giving us $|a^k| = |a^{\gcd(n,k)}|$ and that $|a^k| = \frac{n}{\gcd(n,k)}$ for any finite group. So that for $n = 21$, we have $|a^7| = \frac{21}{\gcd(21,7)} = 3$. So that for any $a \in G \setminus \{e\}$, $|a^7| = 3$. $\square$

12. *Suppose G is a group that contains normal subgroups $H, K \trianglelefteq G$ with $H \cap K = \{e\}$ and $HK = G$. Prove that $G \cong H \times K$.*

Proof. Let G be a group with normal subgroups H, K, such that $H \cap K = \{e\}$ and $HK = G$. We will show $H \times K \cong G$ by defining an function, showing it's well-defined on $H \times K$ to G, that it's a homomorphism and that it's bijective, and hence an isomorphism.

Define $\phi : H \times K \to G$ with the map $(h, k) \mapsto hk$. To show this is well-defined we'll show that this is defined on its domain and its range is contained in its codomain, and that if $((x, y), xy), ((a, b), xy) \in \phi$, then $(a, b) = (x, y)$. Any element in $H \times K$ is an ordered pair of the form (h, k) with $h \in H$ and $k \in K$, and since H, K are subgroups of G we have $hk \in G$. Then take $((x, y), xy), ((a, b), xy) \in \phi$ so that $\phi(x, y) = xy = \phi(a, b)$. By the definition of ϕ and that $H \cap K = \{e\}$ we have that the representation xy is unique for $x \in H$ and $y \in Y$, so that $a = x, y = b$. Hence $((x, y), xy) = ((a, b), xy)$. Thus ϕ is a well-defined map.

To show ϕ is a homomorphism, let $a, b \in G$ so that there exist $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $a = h_1k_1$ and $b = h_2k_2$, and also remember that H and K are normal, so that for any $g \in G$ if $k \in K$ ($h \in H$), then $gkg^{-1} \in K$ ($ghg^{-1} \in H$), then consider the following:

$$\begin{aligned}
\phi(ab) &= \phi((h_1k_1)(h_2k_2)) \\
&= \phi((h_1k_1h_2k_1^{-1})k_1k_2) \\
&= \phi(h_1h_2(h_2^{-1}k_1h_2k_2))
\end{aligned}$$

So we'll get:

$$\begin{aligned}
(h_1k_1h_2k_1^{-1}, k_1k_2) &= (h_1h_2, h_2^{-1}k_1h_2k_2) \\
&\implies \\
h_1k_1h_2k_1^{-1} &= h_1h_2 \\
k_1k_2 &= h_2^{-1}k_1h_2k_2 \\
&\implies \\
h_2k_1 &= k_1h_2
\end{aligned}$$

So the middle terms commute and we get that:

$$\begin{aligned}
\phi(ab) &= \phi(h_1k_1h_2k_2) \\
&= \phi(h_1h_2k_1k_2) \\
&= (h_1h_2, k_1k_2) \\
&= (h_1, k_1) \cdot (h_2, k_2) \\
&= \phi(h_1k_1) \cdot \phi(h_2k_2) \\
&= \phi(a) \cdot \phi(b)
\end{aligned}$$

Thus ϕ is a homomorphism.

Now we'll show it's a bijection. Let $\phi(x, y) = \phi(a, b)$, then $xy = ab$, for $x, a \in H$ and $y, b \in K$. If $x \neq a$ and $y \neq b$, then $a^{-1}x = by^{-1}$ but $H \cap K = \{e\}$ so that $a = x$ and $y = b$, thus $\phi(a, b) = \phi(x, y) \implies$

$(a, b) = (x, y)$ and ϕ is injective into G. Let $g \in G$, so since $G = HK$ there exists a $h \in H$ and $k \in K$ such that $g = hk$. Since $H \cap K = \{e\}$, this is a unique representation of g, so that $(h, k) \in H \times K$ and $\phi(h, k) = hk = g$ and $g \in \text{range}(\phi)$ and $G = \text{range}(\phi)$.

Thus ϕ is an isomorphism between $H \times K$ and G, so that $H \times K \cong G$. □

13. *Let R be a commutative ring.*

13.1. *Prove that the set N of all nilpotent elements of R is an ideal.*

Proof. Let R be a commutative ring and N be the set of all nilpotent elements in R. We'll use the two-step ideal test to show N is an ideal in R.

Clearly $0^1 = 0$, so $N \neq \{\}$. Let $a, b \in N$, then there exists non-negative integers n, m such that $a^n = 0$ and $b^m = 0$, where 0 is the additive identity in R. Without loss of generality assume $m \geq n$, and note that for any $k \geq n$ $a^k = 0$ and any $k \geq m$, $b^k = 0$. Then since R is a commutative ring, we may use the binomial theorem for $(a + b)^{m+n+1}$:

$$\begin{aligned}(a+b)^{m+n+1} &= \sum_{k=0}^{m+n+1} a^k b^{m+n+1-k} \\ &= b^{m+n+1} + ab^{m+n} + ... + a^n b^{m-1} + a^{n+1} b^m + ... + a^{m+n-1} b + a^{m+n}.\end{aligned}$$

Each term has a power of $k \geq n$ or $k \geq m$ so that $a^k b^{m+n+1-k} = 0$ for all $k \in \{0, ..., m + n + 1\}$. So that $(a + b)^{m+n+1} = 0$ and $a + b \in N$.

Now we'll show $-b \in N$. We have $b^m = 0$. Note then $b^m = ((-b)(-b))...((-b)(-b)) = 0$, with this occurring m-times, so that $(-b)^{2m} = 0$. Thus $-b \in N$.

So by the two-step subring test N is a subring of R. □

13.2. *Prove that R/N is a ring with no nonzero nilpotent elements.*

Proof. Let R be a ring and N the subgroup of nilpotent elements in R.

First to show that R/N is a ring we'll show that N is an ideal in R.

Let $r \in R$ and $n \in N$ such that for some $m \in \mathbb{N}$ $n^m = 0$. Then $(rn)^m = (rn)...(rn)$, m-times, and since R is commutative, $(rn)^m = r^m n^m = r^m 0 = 0$. So $rn \in N$ for all $r \in R$. Thus R/N is a ring.

Now let $(r + N)^m = 0 + N$ for some $m \in \mathbb{N}$. Then $r^m + N = 0 + N$, hence $r^m \in N$ and r^m is nilpotent. If r^m is potent, that is there exists a $n \in \mathbb{N}$ such that $(r^m)^n = 0 = (r)^{mn}$ hence $r \in N$. Thus $r + N = N$ and the only nilpotent element in R/N is N. □

13.3. *Show that N is contained in every prime ideal of R.*

Proof. Let R be a ring with N the ideal of nilpotent elements in R, and P be any prime ideal of R. That is if $ab \in P$, then $a \in P$ or $b \in P$.

Let $n \in N$. Then there exists some $m \in \mathbb{N}$ such that $n^m = 0$. Since P is a subring of R, we have that $0 \in P$, hence $n^m \in P$. So P is prime, so that either $n^{m-1} \in P$ or $n \in P$. If it's $n \in P$, we're done. If it's $n^{m-1} \in P$, then either $n^{m-2} \in P$ or $n \in P$. If it's $n \in P$, we're done. If it's $n^{m-2} \in P$, then we repeat this process until we get to $n \in P$.

Hence $N \subseteq P$, for any prime ideal P in R. □

14. *Let $z \in \mathbb{C}$ be a complex number and let $\epsilon_z : \mathbb{R}[x] \to \mathbb{C}$ be the evaluation homomorphism given by $\epsilon_z(p(x)) = p(z)$ for each $p(x) \in \mathbb{R}[x]$.*

14.1. *Show that $\ker(\epsilon_z)$ is a prime ideal.*

Proof. Let $z \in \mathbb{C}$ and $\epsilon_z : p(x) \mapsto p(z)$ for all $p(x) \in \mathbb{R}[x]$. Then since this is a homomorphism, $\ker(\epsilon_z)$ is in fact an ideal.

Furthermore, let $q(x)p(x) \in \ker(\epsilon_z)$, then $\epsilon_z(q(x)p(x)) = 0 \implies p(z)q(z) = 0$. Since $\mathbb{C}$ is an integral domain, either $p(z) = 0$ or $q(z) = 0$, hence either $p(x) \in \ker(\epsilon_z)$ or $q(x) \in \ker(\epsilon_z)$. Thus $\ker(\epsilon_z)$ is a prime ideal in $\mathbb{R}[x]$. □

14.2. *Compute $\ker(\epsilon_{1+i}), \text{im}(\epsilon_{1+i})$ and then state the conclusion of the First Isomorphism Theorem applied to the homomorphism ϵ_{1+i}.*

Solution. *$\epsilon_{1+i}(p(x)) = p(1+i)$. If $p(x) \in \ker(\epsilon_{1+i})$, then $p(1+i) = 0$. Note that since $\mathbb{R}$ is a field, $\mathbb{R}[x]$ is a principal ideal domain, that is every ideal in $\mathbb{R}[x]$ is principle. So then $\ker(\epsilon_{1+i})$ is an ideal by (a), hence is generated by a minimal polynomial in $\mathbb{R}[x]$. Everything in $\ker(\epsilon_{1+i})$ has roots at $x = 1+i$ and $x = 1-i$ by the conjugate root theorem. So that the minimal polynomial of $\ker(\epsilon_{1+i})$ is $x^2 - 2x + 2$ and thus $< x^2 - 2x + 2 >= \ker(\epsilon_{1+i})$.*

For $\operatorname{im}(\epsilon_{1+i})$ we have that this is characterized by $\epsilon_{i+1}(p(x)) = p(1+i)$. I'll show that $\operatorname{im}(\epsilon_{1+i}) = \mathbb{C}$.

We already have $\operatorname{im}(\epsilon_{1+i}) \subseteq \mathbb{C}$, so we'll show that $\mathbb{C} \subseteq \operatorname{im}(\epsilon_{1+i})$. Take $z \in \mathbb{C}$, so that $z = a + bi$ for some $a, b \in \mathbb{R}$. Then consider the polynomial in $\mathbb{R}[x]$, $p(x) = bx + (a - b)$, so that $\epsilon_{1+i}(p(x)) = b(1+i) + a - b = a + bi$. Hence $\mathbb{C} \subseteq \operatorname{im}(\epsilon_{1+i})$. Thus $\mathbb{C} = \operatorname{im}(\epsilon_{1+i})$.

By the first isomorphism theorem for rings, this gives us that $\mathbb{R}[x]/ < x^2 - 2x + x >\cong \mathbb{C}$, with $\phi : \mathbb{R}[x]/ < x^2 - 2x + x >\to \mathbb{C}$ given by $\phi(p(x)+ < x^2 - 2x + x >) = \epsilon_{1+i}(p(x)) = p(1+i)$ being an isomorphism between $\mathbb{R}[x]/ < x^2 - 2x + x >$ and $\mathbb{C}$.

15. *Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear transformation that expands radially by a factor of 3 around the parameterized by $L(t) = \begin{bmatrix} 2 \\ 2 \\ -1 \end{bmatrix} t$, leaving the line itself fixed (viewed as a subspace).*

15.1. *Find an eigenbasis for T and provide the matrix representation of T with respect to that basis.*

Proof. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear transformation that expands radially by a factor of 3 around the parameterized line given by $L(t) = \begin{bmatrix} 2 \\ 2 \\ -1 \end{bmatrix} t$, leaving the line itself fixed (viewed as a subspace).

So to find the eigenvalues of this operator, note that $T(2,2,-1)^T = (2,2,-1)$ hence $\lambda_1 = 1$ with $(2,2,-1)^T$ is an eigenpair for T. To find the other values, note that on it's perpendicular to this line T will scale the vector perpendicular to the line by 3, so that we'll find the orthogonal complement of the line $L(t)$ described above.

Note $L(t)^\perp = \operatorname{span}\{(2,2,-1)^T\}^\perp = \{(2,2,-1)^T\}^\perp$ giving us the equation:

$$< (x,y,z)^T, (2,2,-1)^T > = 0$$
$$2x + 2y - z = 0$$

for $x, y, z \in \mathbb{R}$. So that a basis of the orthogonal complement is given by: $\operatorname{span}\{(1,0,2)^T, (0,1,2)^T\}$. Hence we have $T(1,0,2)^T = 3(1,0,2)^T$ and $T(0,1,2)^T = 3(0,1,2)^T$ our final eigenpairs. We know that $(2,2,-1)^T$ is linearaly independent to both $(1,0,2)^T$ and $(0,1,2)^T$ since they have distinct eigenvalues, so we'll just have to check that the two for $\lambda = 3$ are linearaly independent to each other.

$$a(1,0,2)^T + b(0,1,2)^T = (0,0,0)^T$$
$$a = 0$$
$$b = 0$$

so they are linearly independent in $\mathbb{R}^3$ so that the set $\{(2,2,-1)^T, (1,0,2)^T, (0,1,2)^T\}$ are an eigenbasis of T, with matrix representation: $T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$ □

15.2. *Provide the matrix representation of T with respect to the standard basis.*

Solution. $T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$ *so that $T(1,0,0)^T = (1,0,0)^T = a(1,0,2)^T + b(0,1,2)^T + c(2,2,-1)^T$.*

$$a + 2c = 1$$
$$b + 2c = 0$$
$$2a + 2b - c = 0$$

this gives us $a = -3, b = -4, c = 2$. Repeating this process above for $(0,1,0)^T, (0,0,1)^T$ we get the following representation of T with respect to the standard ordered basis: $T = \begin{bmatrix} -3 & -4 & 2 \\ -4 & 5 & 2 \\ 2 & 2 & -1 \end{bmatrix}$.

Spring 2015

16. *Let G and H be groups of order 10 and 15, respectively. Prove that if there exists a nontrivial homomorphism $\phi : G \to H$, then G is abelian.*

Proof. Let G and H be groups with orders $|G| = 10$ and $|H| = 15$. Suppose there's a nontrivial homomorphism $\phi : G \to H$.

Then note that $|\phi(G)|$ divides both $|G|$ and $|H|$, so that $|\phi(G)| = 5$, since ϕ is non-trivial. Additionally by the first isomorphism theorem we have $G/\ker(\phi) \cong \phi(G)$ so that $|G|/|\ker(\phi)| = 5$, hence $|\ker(\phi)| = 2$. So there exists a $g' \in G \setminus \{e\}$ such that $g' \in \ker(\phi)$ and that $(g')^2 = e$. So that for any $g \in G$ we have $g = eg = (g')^2 g \implies g'g = gg'$, hence the center of G, $Z(G) \neq \{e\}$. Moreover $|\phi(Z(G))|$ divides both $|\phi(G)|$ so $|\phi(Z(G))| = 1$ or 5. If $|\phi(Z(G))| = 1$, then $|Z(G)| = 2$ and we have that $Z(G) = \ker(\phi)$. So then $|G/Z(G)| = 5$, and $G/Z(G)$ is cyclic. Thus G is abelian, since if $G/Z(G)$ is cyclic, then G is abelian for finite groups. But $Z(G) \neq G$, a contradiction.

Alternatively, if $|\phi(Z(G))| = 5$, then $|g'| = 2$ and $|\phi(Z(G))| = 5$ divide $|Z(G)|$ hence $|Z(G)| = 10$ and $Z(G) = G$, and G is abelian. □

17. *Let G be an abelian group and G_T be the set of elements of finite order in G*

17.1. *Prove that G_T is a subgroup of G.*

Proof. Let G be an abelian group and G_T be the set of elements of finite order.

Let $a, b \in G_T$. Then there exists $m, n \in \mathbb{N}$ such that $a^m = e = b^n$. Without loss of generality assume $m > n$. So that $(ab)^{mn} = (ab)...(ab)$, mn-times, since G is abelian we may rearrange these so that we have: $a^{mn}b^{mn} = (a^m)^n(b^n)^m = e^n e^m = e$. Hence $ab \in G_T$.

Let $a \in G_T$, so that there's a $n \in \mathbb{N}$ such that $a^n = e$. $a^{-1} \in G$ so that $a...a = e$ (n - times) implies $a...aa^{-1} = a^{-1} \implies a^{n-1} = a^{-1} \implies e = a^{-n} = (a^{-1})^n = e$. Hence $a^{-1} \in G_T$, whenever $a \in G_T$.

Thus G_T is a subgroup of G. □

17.2. *Prove that every non-identity element of G/G_T has infinite order.*

Proof. Let G be an abelian group and G_T be the subgroup of finite order in G.

Let $gG_T \in G/G_T$ be any non-identity element; that is $g \notin G_T$. For sake of contradiction, suppose that gG_T has a finite order, say $|gG_T| = n$. So that $(gG_T)^n = G_T \implies g^n G_T = G_T$. But we assumed that $g^n \notin G_T$, but we have that $g^n \in G_T$, so that for some $m \in \mathbb{N}$, $(g^n)^m = e$, a contradiction of $g \notin G_T$. Thus every non-identity element in G/G_T has infinite order. □

17.3. *Characterize the elements of G_T when $G = \mathbb{R}/\mathbb{Z}$ where $\mathbb{R}$ is the additive group of real numbers.*

Solution. *Note that $r\mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ whenever $r \in \mathbb{R}$. For g to be in G_T when $G = \mathbb{R}/\mathbb{Z}$ we need to have some $m \in \mathbb{N}$ such that $(r\mathbb{Z})^m = \mathbb{Z}$. That is: $r^m\mathbb{Z} = \mathbb{Z}$. So this is the set of real numbers $r \in \mathbb{R}$ such that for some $m \in \mathbb{N}$ we have $r^m \in \mathbb{Z}$, in set builder notation: $G_T = \{r \in \mathbb{R} : \text{for some } n \in \mathbb{N}, r^n z, \text{ where } z \in \mathbb{Z}\}$. In plain language this is the set of all real elements that are the n^{th} roots of the positive integers. With the negative integers this extends into $\mathbb{C}$. This will include all non-negative real numbers, but that's another proof.*

18.

18.1. *Suppose I and J are ideals in a commutative ring with unity R such that $R = I + J$. Prove that the map $f : R \mapsto R/I \times R/J$ given by $f(x) = (x + I, x + J)$ induces the isomorphism*

$$R/IJ \cong R/I \times R/J$$

.

Proof. Let I and J be ideals within a commutative ring with unity R such that $R = I + J$. Define the map $f : R \mapsto R/I \times R/J$ given by $f(x) = (x + I, x + J)$ for all $x \in R$.

We'll show that this is ring homomorphism, that is it preserves order of additive and multiplicative operations of R, $\ker(f) = IJ$ and that $f(R) = R/I \times R/J$.

For ring homomorphism consider the following, let $x, y \in R$:

$$\begin{aligned}
f(x+y) &= ((x+y)+I, (x+y)+J) \\
&= (x+I+y+I, x+J+y+J) \\
&= (x+I, x+J) + (y+I, y+J) \\
f(xy) &= ((xy)+I, (xy)+J) \\
&= (x+I, x+J) \cdot (y+I, y+J).
\end{aligned}$$

thus f is a ring homomorphism between R and $R/I \times R/J$. We'll show $\ker(f) = IJ$. Let $x \in \ker(f)$, then $(x+I, x+J) = (I, J)$, so that $x \in I \cap J$. We may write $x = xe$ where $x \in I$ and $e \in J$, so that $x \in IJ$. Conversely, let $x \in IJ$. That is for some $i \in I$ and $j \in J$ we have $x = ij$. Note both I and J are ideals so that $ij \in I$ and $ij \in J$ hence $f(x) = f(ij) = (ij+I, ij+J) = (I, J)$. Thus $x \in \ker(f)$. So that $\ker(f) = IJ$.

We'll show that $f(R) = R/I \times R/J$. Clearly $f(R) \subseteq R/I \times R/J$, so we'll show the converse. Let $(a+I, b+J) \in R/I \times R/J$ for some $a, b \in R$. Note since $R = I + J$, we have some $i_1, i_2 \in I$ and $j_1, j_2 \in J$ such that $a = i_1 + j_1, b = i_2 + j_2$. This gives us:$a + I = i_1 + j_1 + I = j_1 + I = i_2 + j_1 + I$ and $b+J = i_2+j_2+J = i_2+J = i_2+j_1+J$. Thus $f(i_2+j_1) = (a+I, b+J)$ so that $(a+I, b+J) \in f(R)$. Hence $f(R) = R/I \times R/J$ and by the first isomorphism theorem of rings we have that $R/IJ \cong R/I \times R/J$. $\square$

18.2. *Prove that $\mathbb{Z}_3[x]/(x^3 - x^2 - 1) \cong \mathbb{Z}_3[x]/(x^3 + x + 1)$. (Hint: Use part (a).)*

Proof. Stating some theorem's that'll be used later on: for an irreducible polynomial over a field F, that is $f(x) \in F[x]$ being irreducible, and $a \in E \supseteq F$ such that $f(a) = 0$, where E is some extension of F, we have that $F(a) \cong F[x]/(f(x))$. We'll need to show first that $\mathbb{Z}_3[x] =< (x^3 - x^2 - 1) > + < (x^3 + x + 1) >$, so here we can use the fact that since $\mathbb{Z}_3$ is a field, we have that $\mathbb{Z}_3[x]$ is a principle ideal domain. Hence $\mathbb{Z}_3[x]$ is an ideal of itself, so that $\mathbb{Z}_3[x]$ is generated by a single element and $\square$