Algebra qual study guide

James C. Hateley

1. Linear Algebra

Exercise 1.1. *It is known that real symmetric matrices are always diagonalizable. You may assume this fact.*

(a) What special properties do the eigenspaces of a real symmetric matrix have? State it clearly.
(b) Now use the property stated in (a) to prove that any real symmetric matrix S can be diagonalized by an orthogonal matrix U, that is, there exists an orthongal matrix U so that $U^{-1}SU$ is diagonal.

Proof: For part (a), there are several things to say. First if A is an $n \times n$ real symmetric matrix then A has n real eigenvalues counting multiplicities. For each eigenvalue the dimension of the corresponding eigenspace is equal to the algebraic multiplicity of that eigenvalue. Any two eigenvalues from different eigenspaces are orthogonal and there exists an invertible, orthogonal matrix P such that the matrix PAP^{-1}. Furthermore the vectors in the columns of P form the eigenspace for the matrix A and the diagonal matrix PAP^{-1} is comprised of the corresponding eigenvalues of A.

For part (b), let A be a real symmetric matrix, $\{\lambda_i\}$ be the set of eigenvalues, $\{v_i\}$ be the set of eigenvectors and $\langle \cdot, \cdot \rangle$ be the standard inner product. Now if λ_i and λj are distinct eigenvalues we have

$$\langle \lambda_i v_i, v_j \rangle = \langle A v_i, v_j \rangle = \langle v_i, A^T v_j \rangle = \langle v_i, A v_j \rangle = \langle v_i, \lambda_j v_j \rangle$$

and so we have $\langle \lambda_i v_i, v_j \rangle = \langle v_i, \lambda_j v_j \rangle$, which implies $(\lambda_i - \lambda_j)\langle v_i, v_j \rangle = 0$ since the eigenvalues are real. This implies that $\langle v_i, v_j \rangle = 0$ since $\lambda_i \neq \lambda_j$.

For an a matrix that has eigenvalues with a multiplicity greater than one, the result can be shown by induction on the size of the matrix. Let A be a symmetric $k \times k$ matrix. If $k = 1$, a basis for A consists of only one eigenvector, hence the basis is orthogonal. Now suppose this is true for an arbitrary $k \times k$, that is there is an orthogonal basis of eigenvectors. Take a $k + 1 \times k + 1$ matrix. Choose an arbitrary eigenvector for the matrix. It spans a one dimensional subspace that is A-invariant. Call this subspace W. Then $W^\perp$ is a k-dimensional space that is also A-invariant, and the arbitrary eigenvector previously chosen is perpendicular to this subspace. By the induction hypothesis $W^\perp$ is an orthogonal basis of eigenvectors for k dimensional space and $W^\perp \perp W$ by construction. Let U be the matrix with columns from the basis of W and $W^\perp$. Then all the columns of p are orthogonal and since the columns are comprised of eigenvectors we have $U^{-1}SU$ is a diagonal matrix.

Exercise 1.2. *Find a matrix P such that PCP^{-1} is in rational form if*

$$C = \begin{pmatrix} -1 & -2 & 6 \\ -1 & 0 & 3 \\ -1 & -1 & 4 \end{pmatrix}$$

To save you computation we tell you that the minimal polynomial of C is $(x-1)^2$

Proof: Computing the characteristic equation we have $c_A(x) = (1-x)^3$, and the minimum polynomial $m_A(x) = (x-1)^2$. The elementary divisors are $(x-1), (x-1)$. So the invariant factors are $(x-1)^2$ and $(x-1)$. The rational canonical form is then

$$PCP^{-1} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Now we need to find a basis for the kernal of $(A-I)^2$, multipling this out we see that this is the zero matrix, so a basis is the standard basis. Choose $e_1 = (1,0,0)^T$. We need to find a 2 dimensional

C-invariant space.

$$Ce_1 = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix} \qquad C^2e_1 = \begin{pmatrix} -3 \\ -2 \\ -2 \end{pmatrix} = -e_1 + 2Ce_1$$

So $\{e_1, Ce_1\}$ form a basis for this space. Now solving for the kernal of the last invariant factor $(C - I)$ we have the vectors $v_1 = (-1, 1, 0)^T$, $v_2 = (3, 0, 1)^T$. We need to find a one dimensional C-invariant space, which is easy enough since $Cv_1 = v_1$. So the columns of Q are comprised of the vectors $\{e_1, Ae_1, v_1\}$. Now we have $Q^{-1}CQ$. Let $P = Q^{-1}$, then we have

$$P = \begin{pmatrix} 1 & 1 & -2 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix} \qquad \text{and} \qquad PCP^{-1} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Definition: The companion matrix for a polynomial $p(x) = x^n + \sum_{k=0}^{n-1} a_k x^k$ is the matrix formed from the vectors $\{1, x, x^2, \ldots, x^{n-1}, x_n\}$, where $x_n = -\sum_{k=0}^{n-1} a_k x^k$. i.e

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Theorem: Rational Canonical Form (RCF) Let A be a matrix with entries from a field $\mathbb{F}$. Let $c_A(x)$ be the characteristic polynomial and $m_A(x)$ be the minimum polynomial. Let $\Phi_i(x)$ be the set of invariant factors such that $\Phi_{i-1} | \Phi_i(x)$. Each $\Phi_i(x)$ will divide $m_A(x)$ and $\Pi\Phi_i(x) = c_A(x)$. Let C_i be the corresponding companion matrix to $\Phi_i(x)$. Then the Rational Canonical Form is a direct sum of C_i, i.e, $\bigoplus C_i$.

Let $K_{\Phi_i} = \ker(\Phi_i(A))$ and $b_{i_1} \in K_{\Phi_i}$, then $\beta_i = \{b_{i_1}, Ab_{i_1}, A^2b_{i_1}, \ldots\}$, where $|\beta_i| = \deg(\Phi_i(x))$. Each β_i will be an A-invariant subspace that will form the columns of the change of basis matrix P, such that $P^{-1}AP = RCF$.

The following steps outline how to find the RCF

(a) Determine the characteristic polynomial of A.
(b) Determine the minimal polynomial of A.
(c) From the minimal polynomial and characteristic equation, determine the invariant factors.
(d) Find A-invariant bases associated to each invariant factor.
(e) Form a rational canonical basis from K_{Φ_i} as a disjoint union of these A-invariant subspaces.

Remark: This is given interms of matricies, in terms of a linear operator T, T-cyclic is the same as A-invariant, then everything is the same.

Exercise 1.3.

(a) *Let $T : V \to W$ be a surjective linear transformation of finite dimensional vector spaces over a field $\mathbb{F}$. Show that there is a linear transformation $S : W \to V$ such that $T \circ S$ is the identity map on W.*
(b) *Use (a) to show that every $n \times m$ matrix of rank n with coefficients in a field has a right inverse.*

Proof: For part (a), if T is surjective then for all $w \in W$, there is a $v \in V$ such that $T(v) = w$. In particular, if $\{f_i\}$ is a basis for W then there exists $\{e_i\}$ such that $T(e_i) = f_i$, this can be done by the axiom of choice. Define a linear map $S : W \to V$ that takes $T(f_i) = e_i$. Now by construction $(T \circ S)(f_i) = T(e_i) = f_i$. We can write any $w \in W$ as a linear combination of $\{f_i\}$ and since both S and T are linear we have for all $w \in W$, $(T \circ S)(w) = T(v) = w$, for some $v \in V$. In otherwords $T \circ S = I_W$, the identity map on W.

For part (b), let A be an $n \times m$ matrix over a field $\mathbb{F}$ with rank n. This first implies that $n \geq m$ since the matrix has rank n it has n linearly independent rows. Let a_j represent the columns of A and $\{e_i\}$ be the standard basis for $\mathbb{F}^m$. Consider the linear transformation $T : \mathbb{F}^m \to \mathbb{F}^n$, such that $T(e_i) = a_j$, for i from 1 to $n \leq m$. The matrix representation of this transformation is A. Furthermore the transformation T is surjective. From part (a), and the same construction as part (a), we know that there exists an S such that $S : \mathbb{F}^n \to \mathbb{F}^m$ and $(T \circ S) = I_{\mathbb{F}}^n$. Let B be the matrix representation of the linear transformation S. Then for all $x \in \mathbb{F}^n$, there is a $y \in \mathbb{F}^m$ such that we have $ABx = (T \circ S)x = T(y) = Ay = x$.

Exercise 1.4. *Let $T : V \to W$ be a nontrivial linear transformation between two finite dimensional vector spaces. Prove that there exists basis for V and W so that the matrix representation of T with respect to these bases has an identity matrix in the top left corner and all other entries equal to zero.*

Proof: Let $\dim(V) = n$, $\dim(W) = m$, the base field be $\mathbb{F}$ and fix a basis $\mathcal{B} = \{b_i\}$ for V. Consider the isomorphisms $\tau : V \to \mathbb{F}^n$ and $\sigma : W \to \mathbb{F}^m$. Now consider $c_i = T(b_i)$, if $b_i \in \ker(T)$ then $c_i = 0 \in W$. Denote the set of vectors $\{c_i\} \notin \ker(T)$ by $\{c_j\}$ and extend this set $\{c_j\}$ to a basis for W and call this basis $\mathcal{C}$. Denote A as the matrix representation of T and $\operatorname{rank}(A) = k$. Now denote $A = [[T(e_1)]_\sigma \cdots [T(e_n)]_\sigma]$. Now we have

$$T(c_i) = \sum_{j=1}^{m} a_j c_j = c_i$$

Hence the matrix representation of this transformation with respect to the basis $\mathcal{B}$ and $\mathcal{C}$ is:

$$A = [T]_{\mathcal{B}}^{\mathcal{C}} = \begin{pmatrix} I_k & 0_{k,n-k} \\ 0_{m-k,k} & 0_{m-k,n-k} \end{pmatrix}$$

Exercise 1.5. *Let $A \in M_n\mathbb{C}$ be the matrix where every diagonal entry is 0 and every off-diagonal entry is 1.*

(a) Find the eigenvalues of A.
(b) Find the eigenspaces of A.
(c) Compute $\det(A)$

Proof: For part (a) the eigenvalues will be the roots of $\det(A - \lambda I_n)$. Now applying the column operations $c_i = -c_n + c_i$ for columns 1 to $n-1$ to the matrix $A - \lambda I_n$ will not change the determinant of the matrix. After applying these operations we have:

$$\det(A - \lambda I_n) = \begin{vmatrix} -\lambda - 1 & 0 & \cdots & 0 & 1 \\ 0 & -\lambda - 1 & \cdots & 0 & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -\lambda - 1 & 1 \\ 1 + \lambda & \cdots & 1 + \lambda & 1 + \lambda & -\lambda \end{vmatrix} = (\lambda + 1)^{n-1} \begin{vmatrix} -1 & 0 & \cdots & 0 & 1 \\ 0 & -1 & \cdots & 0 & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & 1 \\ 1 & \cdots & 1 & 1 & -\lambda \end{vmatrix}$$

Now doing the row operations $r_n = r_i + r_n$ starting at row 1 and going to row $n-1$ will not change the determinant. Applying this we have

$$\det(A - \lambda I_n) = (\lambda + 1)^{n-1} \begin{vmatrix} -1 & 0 & \cdots & 0 & 1 \\ 0 & -1 & \cdots & 0 & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & 1 \\ 0 & \cdots & 0 & 0 & -\lambda + n - 1 \end{vmatrix}$$

Since we now have a diagonal matrix the determinant be the product of the diagonal times the factors we took out. So $\det(A - \lambda I_n) = (\lambda + 1)^{n-1}(-\lambda + n - 1)(-1)^{n-1}$. So the eigenvalues are -1 with a multiplicity of $n-1$ and $n-1$.

For part (b) we need to solve the $\ker(A - \lambda I_n)$ using the eigenvalues from part (a). For the eigenvalue

$n-1$ and using the same idea execpt replacing $r_i = r_i + r_n$ for $i = 1..n$ we have

$$\ker(A-\lambda I_n) = \ker\begin{pmatrix} -n & 0 & \cdots & 0 & n \\ 0 & -n & \cdots & 0 & n \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -n & n \\ 1 & \cdots & 1 & 1 & -n+1 \end{pmatrix}$$

We can ignore the last row since it is linearly dependand, so we $nx_i = nx_n$, for $i = 1..n-1$. Letting each $x_n = 1$ we have the vector $(1,1,\ldots 1,1)^T$. For the eigenvalue of -1 we have a matrix full of ones. The corresponding eigenspace is $e_1 + e_i$ for $i = 2..n$, where e_i is a standard basis vector for $\mathbb{R}^n$. Written out the eigen vectors are:

$$\left\{\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \cdots, \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}\right\}$$

For part (c) the operation $r_i = r_i - r_n$ will not change the value of $\det(A)$. Doing this and the row operation $r_n = r_i + r_n$, we have:

$$\det(A) = \begin{vmatrix} -1 & 0 & \cdots & 0 & 1 \\ 0 & -1 & \cdots & 0 & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & 1 \\ 1 & \cdots & 1 & 1 & 0 \end{vmatrix} = \begin{vmatrix} -1 & 0 & \cdots & 0 & 1 \\ 0 & -1 & \cdots & 0 & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & 1 \\ 0 & \cdots & 0 & 0 & n-1 \end{vmatrix} = (-1)^{-1}(n-1)$$

Exercise 1.6. *Let V be a finite dimensional vector space, let $T : V \to W$ be a linear operator and let λ be an eigenvalue of T.*

(a) Carefully define the geometric multiplicity of λ.
(b) Carefully define the algebraic multiplicity of λ.
(c) Prove that the geometric multiplicity of λ is less than or equal to its algebraic multiplicity.

Proof: For part (a), if λ is an eigenvalue for a linear operator, then and $\{\beta_i\}_\lambda$ is a basis for the eigenspace corresponding to λ, then the geometric multiplicity is the dimension of the eigenspace associated to λ, or the size of $|\{\beta_i\}_\lambda|$

For part (b), if λ is an eigenvalue and $c_T(x)$ is the characteristic equation of the linear operator T, then the algebraic multiplicity is the largest exponent of the factor $(x-\lambda)$ that divides $c_T(x)$.

For part (c), let $\dim(V) = n$ and let $\{v_i\}_{i=1}^k$ be a basis for the eigenspace corresponding to the eigenvalue λ. Using the standard basis for V, $\mathcal{E}$, let A be the matrix representation of T, denote $b_i = \{[v_i]_\mathcal{E}\}_{i=1}^k$. Now since b_i are eigenvectors we have an P $n \times n$ matrix such that the first k columns are b_i and in the product PAP^{-1} we have the first k columns as λ down the diagonal and zeros elsewhere. Now

$$\det(PAP^{-1} - \lambda I_n) = \det(P(A-\lambda I_n)P^{-1}) = \det(P)\det(A-\lambda I_n)\det(P^{-1}) = \det(A-\lambda I_n)$$

and $c_T(x) = \det(PAP^{-1} - \lambda I_n)$ contains the factor $(x-\lambda)^k$. So the algebraic multiplicity is at least as large as the geometric multiplicity. Now if $\{\lambda_j\}$ is the set of eigenvalues and $\{v_i\}_j$ are corresponding basis for the eigenspaces, doing the similar steps we see that

$$c_T(x) = \prod_{j=1}(x-\lambda_j)^{k_j} g(x)$$

where k_j is the dimension of the eigenspace corresponding to the eigenvalue λ_j. So we have $\sum_{j=1} k_j \leq n$ since $\deg(c_T(x)) = n$. Now since each algebraic multiplicity is at least as large as the geometric multiplicity we can conclude that the geometric multiplicity for each eigenvalue λ_j is less than or equal to its algebraic multiplicity.

Exercise 1.7. *Consider a real vector space $V = \mathbb{R}^n$ with the Euclidean inner product, and let U be a subspace of V.*

(a) Prove that U has an orthonormal basis.
(b) Find an orthonormal basis for the space of $(1,2,0)^T$ and $(1,1,3)^T$ inside $\mathbb{R}^3$.

Proof: For part (a), let $\{u_i\}$ be a basis for U. Define $w_1 = u_1$ and

$$w_i = u_i - \sum_{k}^{i-1} \frac{\langle u_i, u_k \rangle}{\|u_k\|^2} u_k, \qquad \hat{w}_i = \frac{w_i}{\|w_i\|}$$

The claim is that the set $\hat{w}_i$ is an orthonormal basis for U. By construction, $\|\hat{w}_i\| = 1$ so all that needs to be shown is that the set $\{w_i\}$ is mutually orthongonal. To prove this proceed by induction on the size of U with a minor change to w_i. Let $\dim(U) = n$, if $n = 1$, then $\hat{w}_1$ spans U and $\|\hat{w}_1\| = 1$ hence it is an orthonormal basis. Suppose this is true for $n = m$, that is the set $\{w_i\}$ is mutually orthongonal. Let $n = m+1$, now since $\langle w_i \rangle = \langle u_i \rangle$ for $i = 1..m$ define w_{m+1} as:

$$w_{m+1} = u_{m+1} - \sum_{k}^{m} \frac{\langle u_{m+1}, w_k \rangle}{\|w_k\|^2} w_k$$

Now

$$\langle w_{m+1}, w_i \rangle = \langle u_{m+1} - \sum_{k=1}^{m} \frac{\langle u_{m+1}, w_k \rangle}{\|w_k\|^2} w_k, w_i \rangle = \langle u_{m+1}, w_i \rangle - \sum_{k=1}^{m} \frac{\langle u_{m+1}, w_k \rangle}{\|w_k\|^2} \langle w_k, w_i \rangle$$

but $\langle w_k, w_i \rangle = \delta_{ik}$ so we have

$$\langle w_{m+1}, w_i \rangle = \langle u_{m+1}, w_i \rangle - \frac{\langle u_{m+1}, w_i \rangle}{\|w_i\|^2} \langle w_i, w_i \rangle = 0$$

hence $w_{m+1} \perp w_i$ for $i = 1..m$. So we have $w_i \perp w_j$ for $i \neq j$ and therefore, by induction $\{\hat{w}_i\}$ is an orthonormal basis for U. For part (b), let $u_1 = (1,2,0)^T$ and $u_2 = (1,1,3)^T$ applying the Gram-Schmidt process we have $w_1 = u_1$ and

$$w_2 = u_2 - \frac{\langle u_2, u_1 \rangle}{\|u_1\|^2} u_1 = \frac{1}{5}(2,-1,15)^T$$

Let $\hat{w}_1 = \frac{1}{\sqrt{5}}(1,2,0)^T$, $\hat{w}_2 = \frac{5}{\sqrt{230}}(2,-1,3)^T$. Then we have $\langle \hat{w}_1, \hat{w}_2 \rangle = 0$ and each $\|\hat{w}_i\| = 1$. Furthermore since $\hat{w}_2$ is a linear combination of the original two vectors we have $\langle \{\hat{w}_i\} \rangle = \langle \{u_i\} \rangle$.

Exercise 1.8. *Let V be a finite dimensional vector space. Prove that there exists a basis for V such that projection transformation with repsect to this basis is a diagonal matrix all of whose diagonal entries are zeros and ones.*

Proof: Let T be a projection operator from V to V. If $v \in V$ then we have $T(v) = w \in V$, also $T^2(v) = T(w) = w$ since V is a projection operator. This implies that for any $v \in V$ we have $T^2(v) = T(v)$. In otherwords, $(T^2 - T) = 0$. Hence we have the minimal polynomial as $m_T(x) = x(x-1)$. This means that the characteristic equation $c_T = x^m(x-1)^n$ for some $n, m > 0$. Now recall a theorem about diagonalization, a matrix or linear map is diagonalizable over the field $\mathbb{F}$ if and only if its minimal polynomial is a product of distinct linear factors over $\mathbb{F}$. Hence this operator is diagonal. So there is a matrix P, whose columns are the eigenvectors of the eigenvalues 1 and 0 such that if A is the matrix representation with repect to the standard basis of T, we have

$$PAP^{-1} = \begin{pmatrix} I_n & 0_{n,m} \\ 0_{m,n} & 0_{m,m} \end{pmatrix}$$

In otherwords, the matrix repesentation of T with repsect to the basis of eigenvectors is a diagonal matrix all of whose diagonal entries are zeros and ones.

Exercise 1.9. *Let V be a finite fimensional vector space over $\mathbb{C}$.*

(a) Carefully define the characteristic polynomial of a linear transformation of V and the minimal polynomial of a linear transformation of V.

(b) *Give an example of two linear operators $S : V \to V$, $T : V \to V$ such that S and T have the same characteristic polynomial but are not similar.*

(c) *Given an example of two linear operators such that the operators have the same minimal polynomial but are not similar.*

Proof: For part (a), the characteristic polynomial of an operator $c_T(x)$ is the monic polynomial whose roots are the eigenvalues of the operator. If A is the matrix representation of T with repect to the standard basis then the characteristic polynomial can be given by $c_T(x) = \det(xI_n - A)$. The minimal polynomial $m_T(x)$ is the monic polynomial of least degree such that $m_T(T) = 0$. Furthermore for any other polynomial $p(x)$ such that $p(T) = 0$ we have the $m_T|p(x)$.

For part (b), two linear operators can have the same characteristic polynomial and not be similar if their minimal polynomials are different. Consider the matricies;

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and let these two matricies be the matrix representations of two linear operators. It is easy enough to see that $c_A(x) = c_B(x) = (x-1)^2$. Computing $\ker(xI_2 - A)$ and $\ker(xI_2 - B)$ we have the $m_A(x) = (x-1)$ and $m_B(x) = (x-1)^2$. Hence matricies A and B are not similar. For part (c), consider the matricies;

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The minimal polynomial for A and B is easily computed to be $m_A(x) = m_B(x) = x - 1$, but the dimensions of A and B are not equal, therefore they cannot be similar.

2. Group Theory

Exercise 2.1.

(a) *If G is a finite group of even order, show that G has an element of order 2.*

(b) *Show that if G is a group of order $2k$ where k is odd, then G has a subgroup of index 2.*

Proof: For part (a), suppose G is a finite group with even order and no elements of order 2. Then for all $x \neq 1$ in G we have $x \neq x^{-1}$ since there are no elements or order 2. Each non identity element must have an inverse that is not itself. Pick an non identity element and call it x_1, then $x_1 \neq x_1^{-1}$, pick another non identity element $x_2 \in G/\{x_1, x_1^{-1}\}$, then x_2 will have an inverse that is not itself. Enumerating G in this fashion we have

$$G = \{1, x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots, x_k, x_k^{-1}\}$$

Counting the elements G has $2k + 1$, which is odd for any $k \in N$. Thus one element in G must be its own inverse, i.e. G must have an element of order 2.

For part (b), let $\pi : G \to S_{|G|}$ be permutation representation of the group action such that $\pi_x(g) = x \cdot g$ for $x, g \in G$. Since 2 is prime, by Cauchy's Theorem, G has an element of order 2. Now if x is an element of order 2 and $|G|/2 = k$ is odd then π_x is an odd permutation. To see this notice that π_x is a product of k 2-cycles, hence $\operatorname{sgn}(\pi_x) = -1$. Now consider the sign mapping $\epsilon : \operatorname{Im}(\pi) \to \{\pm 1\}$. This mapping is surjective since $\pi_x \in \operatorname{Im}(\pi)$ and π is odd. Now, by the Fundamental Theorem of Homomorphisms $\operatorname{Im}(\pi)/\ker(\epsilon) \cong \{\pm 1\} \cong \mathbb{Z}_2$. Hence that $[\operatorname{Im}(\pi) : \ker(\epsilon)] = [G : \ker(\epsilon)] = 2$. Therefore G has a subgroup of index 2.

Theorem: (Lagrange's Theorem) If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.

Theorem: (Cauchy's Theorem) If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

Theorem: (Sylow) If G is a finite group of order $p^\alpha m$, where p is prime and does not divide m.

(a) Sylow $p-$subgroups of G exist, i.e. $\text{Syl}_p(G) \neq \emptyset$.
(b) Any two Sylow p-subgroups of G are conjugate in G.
(c) the number of Sylow p-subgroups of G is of the form $1 + kp$, i.e $n_p \equiv 1 \mod p$. Furthermore n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, hence n_p divides m.

Exercise 2.2. *Recall that a transitive subgroup G of S_n is a subgroup with the property that for every i, j with $1 \leq i, j \leq n$ there exists $\sigma \in G$ with $\sigma(i) = j$.*

(a) show that for any i, j with $1 \leq i, j \leq n$ that the stabilizers $\text{stab}(i)$ and $\text{stab}(j)$ are conjugate in G.
(b) Show that the index of $\text{stab}(i)$ in G is n.
(c) Show that neither $\text{stab}(i)$ nor any proper subgroup of $\text{stab}(i)$ is normal in G.

Proof: For part (a) we will show double inclusion $\text{stab}(i)$ and $\text{stab}(j)$ are conjugates. to show that let $\sigma \in \text{stab}(j)$. Since G is transitive there exists a $\tau \in G$ such that $\tau(i) = j$.
$(\subseteq)$ Now consider $\tau^{-1}\sigma\tau \cdot i$;

$$\tau^{-1}\sigma\tau \cdot i = \tau^{-1}\sigma \cdot j = \tau^{-1} \cdot j = i$$

So we have $\tau^{-1}\sigma\tau \in \text{stab}(i)$, hence $\sigma \in \tau\,\text{stab}(i)\tau^{-1}$.

$(\supseteq)$ Now if $\sigma \in \tau\,\text{stab}(i)\tau^{-1}$, then we have

$$\tau\sigma\tau^{-1} \cdot j = \tau\sigma \cdot i = \tau\sigma \cdot i = \tau \cdot i = j$$

So $\tau\sigma\tau^{-1} \in \text{stab}(j)$, hence $\sigma \in \tau^{-1}\,\text{stab}(i)\tau$. In otherwords $\text{stab}(i) = \tau^{-1}\,\text{stab}(j)\tau$ or $\text{stab}(i)$ and $\text{stab}(j)$ are conjugates.

For part (b) first recall the orbit-stabilizer theorem. If G is a group which acts on a finite set S and $s \in S$, then

$$|\,\text{orb}(s)| = [G : \text{stab}(s)] = \frac{|G|}{|\,\text{stab}(s)|}$$

Since G is transtive, for an element i, and every number $1 \leq j \leq n$, there is a $\tau \in G$ such that $\tau \cdot i = j$. This means that G only has one orbit. Since S_n is a permuation on n numbers, the size of $|\,\text{orb}(i)| = n$. Hence we have as a direct consequence of the orbit-stabilizer theorem; $|\,\text{orb}(i)| = [G : \text{stab}(i)] = n$ or the index of $\text{stab}(i)$ in G is n.

For part (c), since the group action is transitive in part (a) we have shown all stabilizers are conjugate to one another. If a stabilizer or any subgroup of a stabilizer is normal, then all elements of $\{1, \ldots, n\}$ have the same stabilizer. In other words if g fixes i, then it fixes all integers from 1 to n. This implies that the action is regular; which means for every i, j, there is a unique $\tau \in G$ such that $gi = j$. In particular, we have $|G| = |S|$ which cannot be true unless $n = 1$ or 2, if which is the case the result is trivial.

Definition: Let A is a nonempty set in G and S be a set, the set of elements $C_G(A) = \{g \in G : gag^{-1} = a, \forall a \in A\}$ is called the centralizer of A in G. The set $N_G(A) = gAg^{-1} = \{gag^{-1} : a \in A\}$ is the normalizer of A in G and the set $Z(G) = \{g \in G : gxg^{-1} = x, \forall x \in G\}$ is called the center of G. If s is a fixed element of a set S, the set $G_s = \{g \in G : g \cdot s = s\}$ is the stabilizer of s in G.

Exercise 2.3.

(a) Give two examples of non abelian and non-isomorphic groups of order 48.
(b) Show that a group of order 48 cannot be simple.

Proof: For part (a), $48 = 2^4 * 3$ if a group is to be non abelian and of order 48, then it cannot be a direct product of cyclic groups. Consider each of the following:

$$A_4 \times \mathbb{Z}_4, \quad S_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \rtimes \mathbb{Z}_4 \times \mathbb{Z}_3 \quad Q_8 \times \mathbb{Z}_6$$

There are more buy permuting the direct products of $\mathbb{Z}_p$. Each group listed above is of order 48, ($|A_4| = 12, |S_4| = 24, |\mathbb{Z}_4 \rtimes \mathbb{Z}_4| = 16, |Q_8| = 8$) and each are can be shown to be non-isomoprhic.

For part (b), let $P_i \in \text{Syl}_2$ and $E = \{P_i\}$ be the set of Sylow 3 subgroups. By Sylows theorem $n_2 = |E| = 1, 3$. If $n_3 = 1$, we're done because there is a unique Sylow 2 subgroup that is normal in G. Otherwise $n_2 = 3$, first we have

$$K = \bigcup_{P_i \in \text{Syl}_3} N(P_i) \lhd G.$$

To see this, let $\tau : E \to S_{n_3}$, where $n_3 = 4, 16$. Now

$$\ker(\tau) = \{g \in G : P_i^g = P_i, forallP_i \in E\} = K$$

It is clear that τ is a homomorphism from G to S_3 and the kernels of homomorphism are normal subgroups, hence $K \lhd G$. We need to show that $1 < |K| < |G|$ for any group of order 48. First $G/K \cong \text{Im}(\tau)$ and hence

$$|G|/|K| \leq |S_2| = 2 \quad \Rightarrow \quad \frac{2^4 \cdot 3}{2!} = 24 \leq |K|.$$

So we have shown $1 < |K| < |G|$, i.e. K is a nontrivial normal subgroup of G, so G is not simple.

Exercise 2.4. *Prove that every finite group of order > 2 has a nontrivial automorphism.*

Proof: First consider $Z(G)$, the center of G and $G/Z(G)$, the latter is isomorphic to the inner automorphisms of G, hence if G is not abelian we are done. Now if $Z(G) = G$ then G is abelian, so consider the map $\tau : g \to g^{-1}$. τ is an automorphism and will be non-trivial unless every element of G equals its inverse. If every element of G is of exponent 2. If this is the case, G a vector space over the field of 2 elements and so $G \cong \oplus\mathbb{Z}_2$. Since $|G| > 2$, then there are atleast two copies, so the map that permutes the coordinates is a nontrivial automorphism.

Exercise 2.5.

(a) *Carefully state the Fundamental Theorem of finite abelian groups.*
(b) *Use your fundamental theorem to list the distinct isomorphism classes of abelian groups with p^4q elements, where p and q are distinct primes.*
(c) *Explain which group in your list is isomorphic to the group $\mathbb{Z}_{pq} \oplus \mathbb{Z}_{p^3}$.*

Proof: For part (a) the Fundamental Theorem of finite Abelian groups states that every finite abelian group is an internal group direct product of cyclic groups of prime-power order. As a consequence of this, the number of, terms in the product and the orders of the cyclic groups, are uniquely determined by the group.

For part (b) we have the following:

$$\mathbb{Z}_{p^4q}, \qquad \mathbb{Z}_{p^3q} \oplus \mathbb{Z}_p, \qquad \mathbb{Z}_{p^2q} \oplus \mathbb{Z}_{p^2}, \qquad \mathbb{Z}_{p^2q} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p, \qquad \mathbb{Z}_{qp} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$$

For part (c), let us describe two decompositions using the Fundamental Theorem of finite Abelian groups. First we have a the elementary divisor decomposition, which is states that every finitely generated abelian group G is isomorphic to a direct sum of cyclic groups, i.e.;

$$(\mathbb{Z}^n \oplus) \bigoplus_{j=1}^{t} \bigoplus_{i=1}^{n} \mathbb{Z}_{{p_j}^{\alpha_i}}$$

where the rank of an abelian group $n \geq 0$ and the numbers p_j are prime numbers and for each prime $p_j, \alpha_{i-1} | \alpha_i$.

The invariant factor decomposition is where a finitely generated abelian group G can is written as a direct sum of the form

$$\mathbb{Z}^n \oplus \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_r}$$

where $k_{i-1}|k_i$ and k_i are uniquely determined by G. Note that these are equivalent statements because of the Chinese remainder theorem, which here states that $\mathbb{Z}_m \cong \mathbb{Z}_p \oplus \mathbb{Z}_q$ if and only if p and q are coprime and $m = pq$. The list from part (b) are written in the invariant factor decomposition, and so $\mathbb{Z}_{pq} \oplus \mathbb{Z}_{p^3} \cong \mathbb{Z}_{p^3q} \oplus \mathbb{Z}_p$.

Exercise 2.6.

(a) Let G be a finite group acting on a finite set S. Prove that the size of the orbit of a point s equal to the index of its stablizer. More precisely, let x^G be the orbit of x under the action of G and let G_x be the subgroup of elements in G that fix x. Prove that $|x^G| = [G : G_x]$.

(b) Use part (a) to prove the class equation:

$$|G| = Z(G) + \sum_{g \in I} [G : C(g)]$$

Where $Z(G)$ is the center of G, $C(g)$ is the centralizer of $g \in G$ and I is a set with of distinct representatives from each nontrivial conjugacy class of G.

(c) Use the class equation to prove that every finite p-group has a nontrivial center.

Proof: For part (a), first let $x \in S$ then by definition $G_x = \{g \in G : gxg^{-1} = x\}$ and $x^G\{y \in S : y = gxg^{-1}, g \in G\}$. Now let $y \in x^G$, then there is a $g \in G$ such that $y = gxg^{-1}$. Hence the map $y : gxg^{-1} \to gG_x$ is a map from x^G to the set of left cosets of G_x in G. This map is surjective since for any $g \in G$, x^g is an element of x^G. Also $x^{g_1} = x^{g_2}$ if an only if $g_2^{-1}g_1 \in G_x$ if and only if $g_1G_x = g_2G_x$, hence the map is also injection. Therefore there is a bijection between the index of the stabilizer of x and the size of the orbit of a point x, i.e, $|x^G| = [G : G_x]$.

For part (b), if $x \in Z(G)$, then $x = x^g$ for all $g \in G$. If $|Z(G)| = n$ and $\{K_i\}_{i=1}^m$ are the conjugacy classes of G not contained in the center and let g_i be a representative of each K_i. We have

$$|G| = \sum_{i=1}^{n} 1 + \sum_{i=1}^{m} |K_i| = |Z(G)| + \sum_{i=1}^{m} [G : g_i^G]$$

where the last equality is from part (a).

Exercise 2.7. *Prove that there are at least two non-isomorphic non-abelian groups of order 24. You should carefully describe your groups and explain how you know that they are not isomorphic.*

Proof: Consider the two groups S_4 and D_12, both groups have order 24 and both are non-abelian. To be a little more precise

$$D_{12} = \langle r, s : r^12 = s^2 = 1, rsr = s\rangle, \qquad S_4 = \langle (i, i+1) : i \in [1, 3]\rangle$$

Now D_{12} has an element of order 12, however S_4 does not have an element of order 12. To see the later fact S_4 is a permutation of 4 numbers. the order of the any element in S_4 is the size of each disjoint cycle. Hence the largest order for an element in S_4 is 4. Therefore these two groups cannot be isomorphic. Also by construction for D_{12}, the condition $rsr = s$ makes this group non-abelian and any symmetric groups S_n for $n > 3$ is non-abelian, consider the products $(12)(123) = (13)$ and $(123)(12) = (23)$.

Exercise 2.8.

(a) Use the Fundamental theorem of finite abelian groups to list the distinct isomorphism classes of abelian groups with 144 elements.

(b) Explain which group in your list is isomorphic to the group $\mathbb{Z}_4 \oplus \mathbb{Z}_{36}$.

Proof: For part (a), writing the prime decomposition to 144 we have $2^4 3^2$. The invariant factor decompositions are:

$$\mathbb{Z}_{2^4 3^2}, \quad \mathbb{Z}_{2^3 3^2} \oplus \mathbb{Z}_2, \quad \mathbb{Z}_{2^2 3^2} \oplus \mathbb{Z}_{2^2}, \quad \mathbb{Z}_{2^4 3} \oplus \mathbb{Z}_3 \quad \mathbb{Z}_{2^3 3} \oplus \mathbb{Z}_{2\cdot 3}, \quad \mathbb{Z}_{2^2 3} \oplus \mathbb{Z}_{2^2 \cdot 3}$$
$$\mathbb{Z}_{2^2 3^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_{2\cdot 3} \oplus \mathbb{Z}_{2\cdot 3} \oplus \mathbb{Z}_2, \quad \mathbb{Z}_{2\cdot 3^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_{2\cdot 3} \oplus \mathbb{Z}_{2\cdot 3} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

For part (b), the group that is isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_{36} \cong \mathbb{Z}_{2^2 3^2} \oplus \mathbb{Z}_4$

Exercise 2.9.

(a) Carefully state the Sylow Theorems.
(b) Prove that every group of order 126 has a normal subgroup of order 7.
(c) Prove that every group of order 1000 is not simple.

Proof: For part (a), there are three Sylow theorems, which are;

(a) For any prime factor p with multiplicity n of the order of a finite group G, there exists a Sylow $p-$subgroup of G, of order p^n, i.e. $\mathrm{Syl}_p(G) \neq \emptyset$.
(b) Any two Sylow p-subgroups of G are conjugate in G, i.e, if $P_1, P_2 \in \mathrm{Syl}_p(G)$ then there is a $g \in G$ such that $P_1 = P_2^g$.
(c) The number of Sylow p-subgroups of G is of the form $1 + kp$, i.e $n_p \equiv 1 \mod p$. Furthermore n_p is the index in G of the normalizer $N_G(P)$ (i.e; $n_p = [G : N_G(P)]$) for any Sylow p-subgroup P, hence n_p divides m.

For part (b), $126 = 2 \cdot 3^2 \cdot 7$. Consider the Sylow subgroups of order 7, by Sylow's first theorem we know there is at least one since $\mathrm{Syl}_7(G) \neq \emptyset$. Furthermore $n_7 \equiv 1 \mod 7$ and $n_7 | 18$. These two conditions imply that $n_7 = 1$. Hence there exists a unique Sylow 7 subgroup, hence it is normal in G. To see this let P be the Sylow 7 subgroup and consider $n_p = [G : N_G(P)] = 1$ by definition we have

$$N_G(P) = \{g \in G : gPg^{-1} = P\}.$$

So $G = N_G(P)$, in otherword P is normal in G.

For part (b), $1000 = 2^3 \cdot 5^3$. Consider $P \in \mathrm{Syl}_5$, $n_5 = 1$ by Sylows theorems and hence there is a unique Sylow $5-$subgroup which is normal. Thus, there is no simple group of order 1000.

3. Rings and Fields

Exercise 3.1. *Let $\mathbb{F}$ be a field of characteristic $p > 0$ and c an element of $\mathbb{F}$. If $x^p - c$ has no roots in $\mathbb{F}$, prove that $x^p - c$ is irreducible in $\mathbb{F}[x]$*

Proof: First if $\mathbb{F}$ is a field of characteristic p, then $\mathbb{F}$ has p^n elements for some $n \in \mathbb{Z}^+$. Let $n, m > 0$, $n + m = p$, and suppose that $x^p - c$ factors into two factors

$$x^p - c = (x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)(x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0) = a(x) \cdot b(x)$$

where $\{a_i\}_{i=1}^n \{b_j\}_{j=1}^m \in \mathbb{F}$. Both n, m have to be larger than 2, otherwise we are done since if $(WLOG)$ $n = 1$ then $x - a_0$ would be a factor of $x^p - c$ and hence a_0 would be a root in $\mathbb{F}$, which contradicts to $x^p - c$ having no roots in $\mathbb{F}$. Take a_0, since p is prime and $\mathbb{F}^\times$ is cyclic we have there is an t such that $a_0^p = c^t$. Now since p is prime we have positive integers r, s such that $1 = rp + st$. Now consider the following:

$$(c^r a_0^s)^p = c^{rp} a_0^{sp} = c^{rp} c^{st} = c$$

but $c^r a_0^s \in \mathbb{F}$ this implies that $x^p - c$ has a root in $\mathbb{F}$ which is a contradiction. Hence $x^p - c$ is irreducible in $\mathbb{F}[x]$.

Exercise 3.2. *Suppose $\mathbb{L}$ is a separable extension of a field $\mathbb{F}$ with $[\mathbb{L} : \mathbb{F}] = 2$. Prove that if $f(x) \in \mathbb{F}[x]$ is irreducible over $\mathbb{F}$, then one of the following occurs:*
(i) $f(x)$ remains irreducible in $\mathbb{L}[x]$, or
(ii) $f(x)$ is a product of two irreducible polynomials in $\mathbb{L}[x]$ of equal degree.

Proof: First consider the factorization of $f(x) = q_1(x) \cdots q_m(x)$ in to irreducibles in $\mathbb{L}[x]$. Let α_i be a root of $q_i(x)$ and α_1 be a root of $q_1(x)$. Let K be the splitting field of $f(x)$, so that $\mathbb{L} \subset \mathbb{K}$. Now the degree of the extension is 2 the extension is normal. Also, since the extension is seperable it is Galois. Let G be the Galois group of $\mathbb{L}/\mathbb{F}$. Since the action of G is transitive on the roots of $f(x)$ there exists $\sigma \in G$ such that $\sigma(\alpha_1) = \alpha_i$. Since L is Galois, $\sigma(\mathbb{L}) = \mathbb{L}$, so $\sigma(q_1(x)) \in \mathbb{K}[x]$ is a polynomial that has $\sigma(\alpha_1) = \alpha_i$ as a root. Therefore, $q_i(x)|\sigma(q_1(x))$. Since both are irreducible, we have $\deg(q_i) = \deg(\sigma(q_1)) = \deg(q_1)$. So all irreducible factors of $f(x)$ in $\mathbb{L}$ have the same degree.

Now the degree is equal to the degree of the extension $\mathbb{L}(a_1)/\mathbb{L}$, which is the degree of $q_1(x)$. Let $n = \deg(f(x))$, for the number of factors we have

$$n = [\mathbb{F}(\alpha_1) : \mathbb{F}] = [\mathbb{F}(\alpha_1) : \mathbb{F}(\alpha_1) \cap \mathbb{L}][\mathbb{F}(\alpha_1) \cap \mathbb{L} : \mathbb{F}].$$

Since $\mathbb{L}$ is Galois over $\mathbb{F}$, then $\mathbb{K}(\alpha_1)$ is Galois over $\mathbb{F}(\alpha_1)$. If $\sigma \in Gal(\mathbb{L}(\alpha_1)/\mathbb{F}(\alpha_1))$, then restricting σ to $\mathbb{K}$ gives a homomorphism $Gal(\mathbb{L}(\alpha_1)/\mathbb{F}(\alpha_1))$ to $Gal(\mathbb{L} \cap \mathbb{F}(a))$. If σ restricts to the identity on $\mathbb{K}$, then it must be the identity on $\mathbb{K}(\alpha_1)$, so the map $Gal(\mathbb{L}(\alpha_1)/\mathbb{F}(\alpha_1))$ to $Gal(\mathbb{L} \cap F(a))$ is one-to-one. This implies that $[\mathbb{L}(\alpha_1) : \mathbb{F}(\alpha_1)] = [\mathbb{L} : \mathbb{L} \cap \mathbb{F}(\alpha_1)]$. Now,

$$[\mathbb{L}(\alpha_1) : \mathbb{L} \cap \mathbb{F}(\alpha_1)] = [\mathbb{L}(\alpha_1) : \mathbb{L}][\mathbb{L} : \mathbb{L} \cap \mathbb{F}(\alpha_1)], \quad [\mathbb{L}(\alpha_1) : \mathbb{L} \cap \mathbb{F}(\alpha_1)] = [\mathbb{L}(\alpha_1) : \mathbb{F}(\alpha_1)][\mathbb{F}(\alpha_1) : \mathbb{L} \cap \mathbb{F}(\alpha_1)].$$

Hence we have $[\mathbb{F}(\alpha_1) : \mathbb{F}(\alpha_1) \cap \mathbb{L}] = [\mathbb{L}(\alpha_1) : \mathbb{L}]$. Now

$$n = [\mathbb{F}(\alpha_1) : \mathbb{F}] = [\mathbb{F}(\alpha_1) : \mathbb{F}(\alpha_1) \cap \mathbb{L}][\mathbb{F}(\alpha_1) \cap \mathbb{L} : \mathbb{F}] = [\mathbb{L}(\alpha_1) : \mathbb{L}][\mathbb{F}(\alpha_1) \cap \mathbb{L} : \mathbb{F}] = d[\mathbb{F}(\alpha_1) \cap \mathbb{L} : \mathbb{F}]$$

where $d = deg(q_1)$, also

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{F}(\alpha_i) \cap \mathbb{L}][\mathbb{F}(\alpha_i) \cap \mathbb{L} : \mathbb{F}] = 2$$

So either $[\mathbb{F}(\alpha_i) \cap \mathbb{L} : \mathbb{F}] = 2$ in which case there are two irreducible polynomials of equal degree or $[\mathbb{L} : \mathbb{F}(\alpha_i) \cap \mathbb{L}] = 2$ in which case $f(x)$ remains irreducible of $\mathbb{L}[x]$.

Definition: An extension $\mathbb{E} \supset \mathbb{F}$ is called separable if for every $\alpha \in E$ the minimal polynomial of α over $\mathbb{F}$ is a separable polynomial i.e., has distinct roots.

Exercise 3.3. *(a) Let R be a UFD and d a nonzero element in R. Prove that there is only finitely many principal ideals in R that contain the ideal (d).*

(b) Give an example of a UFD R and a nonzero element $d \in R$ such that there are infintely many ideals in R containing (d).

Proof: For part (a), since R is a UFD we have

$$d = \alpha \prod_{k=1}^{n} p_k^{e_k}$$

where p_k are distinct and $e_k \in \mathbb{N}$ and α is a unit. Relabel this factorization as a product of not necessarily distinct elements, but there are no exponents e_k.

$$d = \alpha \prod_{k=1}^{n} p_k^{e_k} = \alpha \prod_{k=1}^{m} q_k$$

for $m \geq n$ and $m = n$ if and only if each $e_k = 1$. Now consider the following chain.

$$(d) = \left(\alpha \prod_{k=1}^{m} q_k\right) \subset \left(\alpha \prod_{k=1}^{m-1} q_k\right) \subset \cdots \subset (q_1)$$

There are m ideals containing (d), hence there is only finitely many principal ideals in R containing (d).

For part (b) consider the ring $\mathbb{Z}[x]$, this is a UFD with the usual polynomial division since $\mathbb{Z}$ is a UFD. Now consider the following:

$$(2) \subset (2, x^n), n \in \mathbb{N}$$

This is true for all n, hence there are infinitely many ideals in $\mathbb{Z}[x]$ that contain (2).

Exercise 3.4. *Let R be a commutative ring with unity. Show that an ideal M is maximal if and only if for all $r \in R \backslash M$ there exists an $x \in R$ such that $1 - rx \in M$.*

Proof: ($\Rightarrow$) Let M be a maximial ideal then $R \backslash M$ is a field. Let $r \in R \backslash M$ and suppose that for all $x \in \mathbb{R}$, $1 - rx \notin M$. This implies that $1 - rx \in R \backslash M$, in particular $1 - rx = r(r^{-1} - x) \in R \backslash M$ for all $x \in R$. Let $m \in M$ and choose $x = r^{-1} - m$, this can be done since $R \backslash M$ is a field. We now have $1 - rx = r(r^{-1} - x) = rm \in M$ by definition of an ideal. This is a contradiction to $1 - rx \notin M$, hence there is an $x \in R$ such that $1 - rx \in M$.

($\Leftarrow$) Suppose that M is not maximal, and that for all $r \in R \backslash M$ there exists an $x \in R$ such that $1 - rx \in M$. There is a maximal ideal N containing M such that for an $x \notin N$, we have $M \subset N \subset N + (x) = R$. Hence $1 \in N + (x)$ and so $1 = n + rx$ where $n \in N$, $r \in R$, so we have $1 - rx \in N$. Now if $r \in R \in M$, by hypothesis, we have $1 - rx \in M$ and hence $N \subset M$ or $M = N$ i.e M is maximal.

Exercise 3.5. *Let p be a prime, and let $\mathbb{F}_p$ denote the finite field of p elements. Let x be an indeterminate, and set $R_1 = \mathbb{F}_p[x]/(x^2 - 2)$ and $R_2 = \mathbb{F}_p[x]/(x^2 - 3)$. Determine whether or not R_1 and R_2 are isomorphic rings in each case: (a) $p = 5$; (b) $p = 11$.*

Proof: First recall that if an ideal is maximal in a ring, then the quotient is a field, i.e if $f(x) \in \mathbb{F}_p[x]$ is maximal then $\mathbb{F}_p[x]/(f(x))$ is a field. Also we recall that two finite fields with the same number of elements are isomorphic. Now for $p = 5$ we have the following

$$\begin{cases} x^2 - 2 \\ x^2 - 3 \end{cases} \mod 5 \equiv \begin{cases} x^2 + 3 \\ x^2 + 2 \end{cases} \mod 5$$

If these factor in $\mathbb{F}_5$ to $(x + a)(x + b)$, we have the following

$$\begin{cases} a + b = 0ab = 2, 3 \end{cases} \mod 5$$

There is a short list to check, the pairs $(1, 4), (2, 3)$ are the only 2 that will satisfy $a + b = 0 \mod 5$, but $1 \cdot 4 = 4 \mod 5$ and $2 \cdot 3 = 1 \mod 5$. Hence both $x^2 - 2$ and $x^2 - 3$ are irreducible in $\mathbb{F}_5$, hence both R_1 and R_2 are finite fields with the same number of elements so they are isomorphic. For $p = 11$ we have to look at the pairs

$$(1, 11), (2, 9), (3, 8), (4, 7), (5, 6)$$

Now

$$\begin{cases} x^2 - 2 \\ x^2 - 3 \end{cases} \mod 11 \equiv \begin{cases} x^2 + 9 \\ x^2 + 8 \end{cases} \mod 11$$

and we have using a similiar set of equations,

$$1 \cdot 10 = 10 \mod 11, \quad 2 \cdot 9 = 7 \mod 11, \quad 3 \cdot 8 = 2 \mod 11, \quad 4 \cdot 7 = 6 \mod 11, \quad 5 \cdot 6 = 8 \mod 11,$$

Hence we have $x^2 + 8 = (x + 5)(x + 6)$ in $\mathbb{F}_{11}[x]$ and $x^2 + 9$ is irreducible in $\mathbb{F}_{11}[x]$. This implies that R_1 is a field while R_2 is not, hence they cannot be isomorphic.

Exercise 3.6. *Let $\mathbb{F}$ be a splitting field of the polynomial $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$. Find the degree $[\mathbb{F} : \mathbb{Q}]$ and determine the Galois group of the extension $\mathbb{Q} \subset \mathbb{F}$ up to isomorphism.*

Proof: The zeros of $x^4 - 2$ are $2^{1/4}\omega_k$, where $\omega_k = e^{\imath k\pi/2}$ for $k = 0, 1, 2, 3$. First consider $\mathbb{E} = \mathbb{Q}(2^{1/4})$, it is clear that $\imath \notin \mathbb{E}$ and since $x^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's Irreducibility Criterion with $p = 2$ we have $[\mathbb{E} : \mathbb{Q}] = 4$. Let $\mathbb{F} = \mathbb{Q}(2^{1/4}, \imath)$. Then we have

$$[\mathbb{Q}(2^{1/4}, \imath) : \mathbb{Q}] = [\mathbb{Q}(2^{1/4}, \imath) : \mathbb{Q}(2^{1/4})] \cdot [\mathbb{Q}(2^{1/4}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Because the multiplicitive group $\mathbb{F}^\times$ can be generated by two elements $s = \imath$ and $r = 2^{(}1/4)$, it is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_4$, further more we have $srs = r^{-1}$ hence the group is isomophic to D_8 the permutations of a square.