1. Suppose that a group $G$ acts on a set $X$. For a point $x \in X$, let $G_x$ denote the stabilizer subgroup $\{g \in G \mid gx = x\}$.

   a). If $G$ acts transitively on $X$, show that $G_x$ and $G_y$ are isomorphic subgroups of $G$.
   b). If $G_x$ is conjugate to some subgroup $H$ of $G$, show that $H = G_y$ for some $y \in X$.
   c). Prove that if $G$ acts transitively on $X$ and $G_x$ is normal, then $G_x = G_y$ for all $x$ and $y$ in $X$.
   d). Show that if $X$ is finite and $G$ acts transitively, then the cardinality of $X$ is equal to the cardinality of $G/G_x$, where $x \in X$ is any point.

   **Solution.**
   a). Since $G$ acts transitively, there exists $h \in G$ such that $hy = x$. We have
   
   $$g \in G_x \iff gx = x \iff ghy = hy \iff h^{-1}gh = y \iff h^{-1}gh \in G_y.$$  
   If we define $\varphi : G_x \to G_y$ by $\varphi(g) = h^{-1}gh$ then it is easily verified that $\varphi$ is an isomorphism of groups. In particular, we have $G_y = h^{-1}G_xh$.

   b). Suppose that $H = h^{-1}G_xh$. Set $y = hx$. Then $G_y = h^{-1}G_xh = H$ by a).

   c). By a), we have $G_y = h^{-1}G_xh$, and $h^{-1}G_xh = G_x$ because $G_x$ is normal.

   d). Define $\psi : G/G_x \to X$ by $\psi(gG_x) = gx$. This map is well defined because if $gG_x = g'G_x$ for some $g' \in G$, then $g' = gh$ for some $h \in G_y$ and $g'x = ghx = gx$. The function $\psi$ is onto, because $G$ acts transitively. If $gx = g'x$, then $(g')^{-1}gx = x$, so $(g')^{-1}g \in G_x$ and $g'G_x = gG_x$. This shows that $\psi$ is injective. Hence $\psi$ is bijective and $|G/G_x| = |X|$.

2. Let $\lambda$ be a non-zero element of the algebraically closed field $k$, and let $R$ be the ring $k[t]/(t^2(t - \lambda)^3)$. Note that $R$ is also a $k$-vector space in a natural way.

   a). What is the dimension of $R$ over $k$.
   b). Find an explicit basis for the null space (kernel) of the linear transformation of $R$ over $k$ given by multiplication by $(t - \lambda)^3$.
   c). Find the Jordan canonical form for the linear transformation of the vector space $R$ given by multiplication by $t$.

   **Solution.**
   a). The dimension of $R$ is 5, because 5 is the degree of $f = t^2(t - \lambda)^3$. A basis of $R$ is given by $1 + (f), t + (f), t^2 + (f), t^3 + (f), t^4 + (f)$.

   b). Let $T$ be this linear map. Clearly, $t^2 + (f), t^3 + (f), t^4 + (f)$ lie in the kernel $T$, so the kernel has dimension $\geq 3$ and the rank of $T$ is at most $5 - 3 = 2$. Also, $(t - \lambda)^3 + (f)$ and $t(t - \lambda)^3 + (f)$ are linearly independent vectors in the image of $T$, so the rank of $T$ is equal to 2, the dimension of the kernel is equal to 3, and a basis of the kernel is given by $t^2 + (f), t^3 + (f), t^4 + (f)$.

   c). Denote this linear transformation by $S$. By the Chinese Remainder Theorem we have a natural isomorphism $R \to k[t]/(t^2) \oplus k[t]/((t - \lambda)^3)$ given by $t + (f) \mapsto (t + (t^2), t + (t - \lambda)^3))$. 

If we choose the basis $1 + (t^2), t + (t^2)$ in $k[t]/(t^2)$ and $1 + ((t - \lambda)^3), (t - \lambda) + ((t - \lambda)^3), (t - \lambda)^2 + ((t - \lambda)^3)$ then the matrix of $S$ with respect to these bases is:

$$
\begin{pmatrix}
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & \lambda & 0 & 0 \\
0 & 0 & 1 & \lambda \\
0 & 0 & 0 & 1 \\
\end{pmatrix}.
$$

3. Let $M_{n,m}(k)$ be the vector space of $n \times m$ matrices over a field $k$ and consider the “matrix multiplication map”

$$B : M_{n,1}(k) \times M_{1,m}(k) \to M_{n,m}(k)$$

$$
\left( \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \begin{pmatrix} w_1 & \cdots & w_m \end{pmatrix} \right) \mapsto \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \begin{pmatrix} w_1 & \cdots & w_m \end{pmatrix}
$$

a). Prove that the image of $B$ consists precisely of the $n \times m$ matrices of rank at most one.

b). Explain why $B$ is bilinear and use this show that $M_{n,1}(k) \otimes M_{1,m}(k) \cong M_{n,m}(k)$, as vector spaces over $k$.

c). Give (with justification) an explicit element of $k^3 \otimes k^3$ which can not be written as $v \otimes w$ for any $v, w, \in k^3$.

Solution.

a). For matrices $A_1, A_2$ we have

$$\text{rank}(A_1 A_2) \leq \min\{\text{rank}(A_1), \text{rank}(A_2)\}.$$  

Since $\text{rank}(A_1), \text{rank}(A_2) \leq 1$, we have $\text{rank}(B(A_1, A_2)) = \text{rank}(A_1 A_2) \leq 1$. Suppose that $C$ is an $m \times n$ matrix of rank 1, Then there exist an invertible matrix $D$ such that $DC$ is in row echelon form. So

$$DC = \begin{pmatrix} w_1 & w_2 & \cdots & w_m \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$  

If the first column of $D^{-1}$ is $(v_1, v_2, \cdots, v_n)^{tr}$, then $C = (v_1, \cdots, v_n)^{tr}(w_1, \cdots, w_m)$ lies in the image of $B$.

b) It is easy to verify that $B$ is bilinear. So there exists a unique linear map $\hat{B} : M_{n,1}(k) \otimes M_{1,m}(k) \to M_{n,m}(k)$ such that $\hat{B}(A_1 \otimes A_2) = B(A_1, A_2)$. Clearly, every $m \times n$ matrix $C$ is a sum of matrices of rank $1$, namely $C = C_1 + C_2 + \cdots + C_n$ where $C_i$ is the matrix which has 0’s in all rows except row $i$, and the $i$-th row of $C_i$ is the same as the $i$-th row of $C$. This shows that $\hat{B}$ is surjective. The spaces $B_{n,1}(k) \otimes M_{1,m}(k)$ and $M_{n,m}(k)$ both have dimension $mn$. Therefore, $\hat{B}$ is a linear isomorphism.

c). If $n = m = 3$, then we may identify $M_{n,1}(k)$ and $M_{1,m}(k)$ with $k^3$. So we have an isomorphism $\hat{B} : k^3 \otimes k^3 \to M_{3,3}(k)$ by $b)$. Let $C$ be a $3 \times 3$ matrix of rank $> 1$ and let $A = B^{-1}(C)$. Then $A \in k^3 \otimes k^3$ is not a pure tensor: if $A = A_1 \otimes A_2$ then $C = \hat{B}(A) = \hat{B}(A_1 \otimes A_2) = B(A_1, A_2)$ has rank $\leq 1$.  

2
4. Compute the number of abelian groups of order 120, up to isomorphism.

**Solution.** $120 = 2^4 \cdot 3 \cdot 5$. Every abelian group is isomorphic to the product of its $p$-Sylow subgroups. So an abelian group $G$ of order 120 is isomorphic to $G_2 \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ where $G_2$ is the 2-Sylow subgroup. The possibilities for $G_2$ are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/8\mathbb{Z}$, and these are pairwise nonisomorphic. So there are 3 abelian groups of order 120. (We can also write $G$ uniquely in the form $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$ where $d_1 \mid d_2 \mid \cdots \mid d_r$. Then the groups up to isomorphism are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$, $\mathbb{Z}/120\mathbb{Z}$.)

5. If the Galois group of a finite Galois extension $L/K$ is $S_3$, describe explicitly the lattice of intermediate fields. For each intermediate field $F$, specify what the Galois group of $L/F$ is, and whether $F$ is a normal extension of $K$.

**Solution.** The subgroups of $S_3$ are the trivial group $\langle e \rangle$, the group $S_3$ itself and the cyclic subgroups $\langle (1\ 2) \rangle$, $\langle (1\ 3) \rangle$, $\langle (2\ 3) \rangle$ and $\langle (1\ 2\ 3) \rangle$. By the Galois correspondence, the lattice of intermediate fields is:

![Diagram]

For each group $G$, $L^G$ is the fixed field of $G$, and the Galois group of the extension $L/L^G$ is $G$. The normal subgroups of $S_3$ are $\langle e \rangle$, $S_3$ and $\langle (1\ 2\ 3) \rangle$ so the only cases where $F$ is a normal extension of $K$ are $F = L$, $F = K$ or $F = L^{\langle (1\ 2\ 3) \rangle}$.
1. An ideal $I$ in a commutative ring $R$ is said to be radical if $f^n \in I$ implies $f \in I$, for any element $f \in R$ and any positive integer $n$.
   a). State and prove a characterization of the radical ideals of $\mathbb{Z}$, in terms of their generators.
   b). If $I$ and $J$ are radical ideals of $\mathbb{Z}$, prove that $I \cap J$ and $I + J$ are radical. Here, $I \cap J$ is the largest ideal contained in both $I$ and $J$, and $I + J$ is the smallest ideal containing both $I$ and $J$.
   c). Prove or give a counterexample: If $I$ and $J$ are radical ideals in $\mathbb{Z}$, so is $IJ$. Here, $IJ$ is the ideal generated by elements of the form $xy$ where $x \in I$ and $y \in J$.

Solution.
   a). Every ideal in $\mathbb{Z}$ is principal and of the form $(d)$ with $d \geq 0$. We have $e \in (d)$ if and only if $d \mid e$. The ideal $(0)$ is prime because $\mathbb{Z}$ is an integral domain. It follows that $(0)$ is radical. Let $I = (d)$ with $d > 0$. Let $d = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization where $p_1 < \cdots < p_r$ are distinct primes and $k_1, \ldots, k_r$ are positive integers. We claim that $(d)$ is radical if and only if $d$ is square-free, i.e., $k_1 = k_2 = \cdots = k_r = 1$. Suppose that $(d)$ is radical. Let $f = p_1 \cdots p_r$, then $f^n \in (d)$ if $n \geq k_i$ for all $i$. So $f \in (d)$ and $d \mid f$. It follows that $k_1, \ldots, k_r$ are all equal to 1. Conversely, if $d = p_1 \cdots p_r$, and $f^n \in (d)$, then $d \mid f^n$. It follows that every $p_i$ must appear in the prime factorization of $f$, so $d \mid f$ and $f \in (d)$.
   b). If $I = (0)$ or $J = (0)$ then $I + J$ is equal to $J$ or $I$ respectively, and $I + J$ is radical. If $I = (d)$ and $J = (e)$, then $I + J = (f)$ where $f$ is the greatest common divisor of $d$ and $e$. If $d$ and $e$ are squarefree, then so is $f$, and $I + J$ is radical. The intersection of radical ideals is radical in any ring. Suppose that $I$ and $J$ are radical and $f^n \in I \cap J$. Then $f^n \in I$, so $f \in I$. And also $f^n \in J$ so $f \in J$. Therefore $f \in I \cap J$. This shows that $I \cap J$ is radical.
   c). If $I = J = (2)$, then $I$ and $J$ are radical, but $IJ = (4)$ is not radical because $2^2 \in (4)$, but $2 \not\in (4)$.

2. Let $p_1, \ldots, p_n$ be distinct prime integers, and let $K$ be the extension of $\mathbb{Q}$ obtained by adjoining the square roots of these elements.
   a). Describe the Galois group $G$ of $K$ over $\mathbb{Q}$ by giving an explicit set of generators.
   b). Prove that $G$ is abelian, and express it as a direct sum of subgroups of prime power order.

Solution.
   a), b). Let $K_i = \mathbb{Q}(\sqrt{p_i})$ for all $i$. Since $\sqrt{p_i}$ is irrational, $K_i/\mathbb{Q}$ is a field extension of degree 2. This extension is Galois and $\text{Gal}(K_i/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. This group is generated by $\sigma_i$ where $\sigma_i(\sqrt{p_i}) = -\sqrt{p_i}$. Now the composition field $K = K_1K_2 \cdots K_n$ is also a Galois extension over $\mathbb{Q}$. Restriction gives us an injective group homomorphism
   $$\varphi : \text{Gal}(K/\mathbb{Q}) \to \text{Gal}(K_1/\mathbb{Q}) \times \cdots \times \text{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$$
   Suppose that $\varphi$ is not onto. Then there exists a nonzero group homomorphism $\psi : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$ with $\psi \circ \varphi = 0$. This homomorphism is given by $\psi(a_1 + 2\mathbb{Z}, \ldots, a_n + 2\mathbb{Z}) = k_1a_1 + \cdots + k_na_n + 2\mathbb{Z}$ for some $k_1, \ldots, k_n \in \{0, 1\}$. Define $d = \prod_{i=1}^d p_i^{k_i}$. Then $d$ is a squarefree element integer $> 1$. Since $\sqrt{d}$ is fixed under $\text{Gal}(K/\mathbb{Q})$, we have that $\sqrt{d} \in \mathbb{Q}$. This is a contradiction because $\sqrt{d}$ is irrational. It follows that $\varphi$ is onto. So $\varphi$ is an isomorphism and $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$. 
3. Let \( a \) be a real number. Find the rank and signature of the matrix
\[
\begin{pmatrix}
1 & 0 & 1 \\
0 & 1 & 1 \\
1 & 1 & a
\end{pmatrix}
\]
as a function of \( a \). For which values of \( a \) is it positive definite?

**Solution.** The determinants of the upper-left 1 \times 1, 2 \times 2 and 3 \times 3 submatrices are 1, 1, \( a - 2 \). The quotients, are 1, 1/1 = 1, \((a - 2)/1 = a - 2\). If \( a < 2 \), then the signature is 1, 1, -1, if \( a = 2 \) then the signature is 1, 1, 0, and if \( a > 2 \) then the signature is 1, 1, 1. The matrix is positive definite if \( a > 2 \).

4. Give examples of the following:
   a). A UFD \( R \) that is not a PID.
   b). A module \( M \) over a PID that is neither free nor torsion.
   c). A torsion module over a PID which has two submodules \( M \) and \( N \) satisfying \( M \cap N = 0 \) and whose annihilators satisfy \( \text{Ann} \ M \subset \text{Ann} \ N \).

**Solution.**
   a). \( \mathbb{Q}[x, y] \) is a UFD but not a PID. Every polynomial ring over a field is a UFD, but \( \mathbb{Q}[x, y] \) is not a PID, because \((x, y)\) is not principal.
   b). The \( \mathbb{Z} \)-module \( \mathbb{Z} \oplus \mathbb{Z}/2 \) is not torsion, and not free.
   c). Take \( R = \mathbb{Z} \), and the module \( U = M \oplus N \) where \( M = \mathbb{Z}/2 \) and \( N = \mathbb{Z}/4 \). Then \( \text{Ann} \ M = (2), \text{Ann} \ N = (4) \).

5. a). Let \( n \) be a positive integer, and let \( \text{Aut}(\mathbb{Z}/(2^n)) \) be the automorphism group of the cyclic group \( \mathbb{Z}/(2^n) \) of order 2\(^n\). How many elements does \( \text{Aut}(\mathbb{Z}/(2^n)) \) have?
   b). Suppose that a finite group \( G \) has a cyclic 2-Sylow subgroup \( H \). Show that the centralizer subgroup \( Z_G(H) \) of \( H \) in \( G \) is equal to the normalizer subgroup \( N_G(H) \) of \( H \) in \( G \).

**Solution.**
   a). The group \( \mathbb{Z}/2^n \mathbb{Z} \) is generated by \( 1 + 2^n \mathbb{Z} \). Any automorphism of \( \mathbb{Z}/2^n \mathbb{Z} \) sends \( 1 + 2^n \mathbb{Z} \) to another generator \( a + 2^n \mathbb{Z} \) where \( a \) is odd. There are \( 2^{n-1} \) odd numbers between 0 and \( 2^n \), so \( \text{Aut}(\mathbb{Z}/2^n \mathbb{Z}) \) has \( 2^{n-1} \) elements.
   b). \( H \) is isomorphic to \( \mathbb{Z}/2^n \mathbb{Z} \) for some positive integer \( n \). The group \( Z_G(H) \) acts on \( H \) by conjugation. So we have a group homomorphism
   \[
   \varphi : N_G(H) \to \text{Aut}(\mathbb{Z}/2^n \mathbb{Z}).
   \]
The kernel of \( \varphi \) is \( Z_G(H) \). So \( N_G(H)/Z_G(H) \) can be identified with a subgroup of \( \text{Aut}(\mathbb{Z}/2^n \mathbb{Z}) \). In particular, \( N_G(H)/Z_G(H) \) is a 2-group. If \( N_G(H)/Z_G(H) \) is nontrivial, then 2 divides \( |N_G(H)|/|Z_G(H)| \), so it divides
\[
\frac{|G|}{|H|} = \frac{|G|}{|N_G(H)|} \cdot \frac{|Z_G(H)|}{|N_G(H)|} \cdot \frac{|N_G(H)|}{|Z_G(H)|}.
\]
But \( |G|/|H| \) is odd because \( H \) is the 2-Sylow subgroup of \( G \). Contradiction. So \( N_G(H) = Z_G(H) \).