1. a. We have seen that a finite multiplicative subgroup of a field is cyclic. Show this fails for a commutative ring. If possible, find a counterexample for an integral domain.

Consider the 4 element group \(\{\pm 1, \pm i\}\) in \(\mathbb{Z} \oplus \mathbb{Z}\), which is isomorphic to the Klein 4-group. It cannot happen for an integral domain. A finite subgroup of units is also a finite subgroup in the field of fractions, hence is cyclic.

b. Let \(\phi: \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}\) be a module homomorphism (of \(\mathbb{Z}\)-modules). Show that if \(\phi\) is surjective, it must be injective. Give an example to show that the converse is false—a difference between free \(\mathbb{Z}\)-modules and vector spaces. (You may, of course, think of \(\phi\) as a \(2 \times 2\) matrix with integer entries.)

Let \(A\) be the \(2 \times 2\) matrix representing \(\phi\) (via left multiplication of column vectors). Since \(\phi\) is surjective, there are column vectors of integers mapping to \((1 0)^T\) and \((0 1)^T\), which we can put together to make a matrix \(B\) with \(AB = I\). But then \(\det A\) must be \(\pm 1\), hence \(A\) is invertible as a matrix over \(\mathbb{Z}\) and \(\phi\) is an invertible linear transformation.

For the converse, consider the linear transformation given by the matrix \(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\).

c. Find an example of a \(\mathbb{Z}\)-module \(M\) and surjection \(\phi: M \to M\) which is not injective.

\(M = \mathbb{Q}[x]\) works with \(\phi\) defined as differentiation.

2. Prove that an integral domain \(R\) is a UFD if and only if every nonzero prime ideal contains a principal prime ideal (a nonzero principal ideal which is prime). [Hint: for \((\Leftarrow)\), let \(S\) be the set of all products of prime elements. Let \(c \neq 0\) be a nonunit which is not in \(S\). Use Zorn’s lemma to get a prime ideal \(P \supseteq (c)\) with \(P \cap S = \emptyset\), contradicting the hypothesis.]

\((\Rightarrow)\) Let \(I\) be any nonzero prime ideal, \(0 \neq x \in I\). Since \(I\) is prime, some irreducible factor \(y\) of \(x\) must lie in \(I\). In a UFD, irreducible elements are prime, hence \((y)\) is a principal prime ideal contained in \(I\).

\((\Leftarrow)\) Following the hint, let \(S\) be the set of all products of prime elements. Let \(c \neq 0\) be a nonunit which is not in \(S\). Let \(\mathcal{M}\) be the set of all ideals containing \((c)\) with empty intersection with \(S\). Order \(\mathcal{M}\) by inclusion. Unions of such ideals are again in \(\mathcal{M}\), so any
5. For finite abelian groups, show that if an integer $n$ divides $|G|$, then $G$ has a subgroup of order $n$.

This can be done directly from the Fundamental theorem of finite abelian groups. Another way is to use the fact that $G$, being nilpotent, can be written as a direct product of its Sylow $p$-subgroups for each prime $p$. For each such $p$, there is a subgroup of order $p^r$ where $p^r$ exactly divides $k$ by the first Sylow theorem. The product of these groups gives a subgroup of order $k$. Thus we actually have a stronger theorem.

6. Let $K$ be a field of characteristic $p > 0$, and let $c \in K$. Show that if $\alpha$ is a root of $f(x) = x^p - x - c$, so is $\alpha + 1$. Prove that $K(\alpha)$ is Galois over $K$ with group either trivial or cyclic of order $p$.

$$f(\alpha + 1) = (\alpha^p + 1) - (\alpha - 1 - c) = \alpha^p - \alpha - c = f(\alpha).$$
Therefore, if $\alpha$ is a root of $f$, so is $\alpha, \alpha + 1, \ldots, \alpha + p - 1$, the $p$ distinct roots of $f$. Thus $K(\alpha)$ is both normal and separable (hence Galois) over $K$. If $\alpha \in K$, the Galois group is trivial. Otherwise, it is cyclic of order $p$, generated by $\alpha \mapsto \alpha + 1$. We know this is the whole Galois group since the fixed field of this automorphism is $K$, or because it has order equal to $p = [K(\alpha) : K]$. 

3. Show that the only idempotents in a local ring are 1 and 0.

If $x^2 = x$, then $x(x - 1) = 0$. Either $x$ or $x - 1$ must lie in the maximal ideal (since it is prime), so the other is a unit since it is not in the maximal ideal (otherwise $1 = x - (x - 1)$ is in the maximal ideal). If $x$ is a unit then $x - 1 = 0$ and if $x - 1$ is a unit, then $x = 0$.

4. Let $R$ be an integral domain containing a field $k$ as a subring. Suppose $R$ is a finite dimensional vector space over $k$. Show that $R$ is a field.

Let $n = \dim_k R$ and $0 \neq x \in R$. The set $\{1, x, \ldots, x^n\}$ is linearly dependent, so there is an equation $\sum_{i=0}^{n} a_i x^i = 0$ with $a_i \in k$ not all zero. We may divide by $a_0$ to assume that $a_0 = 1$. Then $1 = x(-a_1 - \cdots - a_{n} x^{n-1})$ so $x$ has an inverse in $R$.

a. Show this is false if $R$ has zero divisors.

Take $R = k[x]/(x^2)$, two dimensional over $k$. 

5. For finite abelian groups, show that if an integer $k$ divides $|G|$, then $G$ has a subgroup of order $k$.
a. Find all subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ with proof that you have them all. What is the minimal polynomial of $\sqrt{2} + \sqrt{3}$? Which of your subfields does it generate over $\mathbb{Q}$?

All subfields are $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, corresponding to the subgroups $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, $\langle(1,0)\rangle$, $\langle(0,1)\rangle$, $\langle(1, 1)\rangle$, $\langle(0)\rangle$ of $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$. The minimal polynomial of $\sqrt{2} + \sqrt{3}$ is $(x - (\sqrt{2} + \sqrt{3}))(x - (-\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))(x - (-\sqrt{2} - \sqrt{3})) = x^4 - 10x^2 + 1$. This polynomial is irreducible over $\mathbb{Q}$ (check), so it generates the extension of degree 4, namely $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

7. Let $L$ be a Galois extension of $K$ with $\text{Gal}(L/K) \cong A_5$, the alternating group of order 60. Let $f \in K[x]$ be an irreducible polynomial of degree 2, 3 or 4. Show that $f$ cannot split in $L$. What can you say if $f$ has larger degree?

If $f$ splits in $L$, its roots generate a normal extension of $K$. Since $f$ was irreducible, this is a nontrivial extension of $K$. Since $f$ has degree less than 5, the extension is of degree at most $4! = 60$, whence $L$ contains a proper normal extension of $K$. But $A_5$ is simple, so it has no proper normal subgroup, a contradiction. If $\deg f > 5$, $f$ may split but no prime greater than 5 can divide the degree. Also $\deg f \leq 60$. 