(1) Take $R=\mathbf{Z}$. Suppose that $M$ is a submodule of $\mathbf{Z}^{n}$ of finite index: the quotient $\mathbf{Z}^{n} / M$ is finite. Here is an explicit way of finding a basis for $M$ :

Choose $v_{1}, \ldots, v_{n} \in M$ such that the determinant of the matrix with rows $v_{1}, \ldots, v_{n}$ is minimal (amongst nonzero possibilities for this determinant). Prove that $M$ is free on $v_{1}, \ldots, v_{n}$. ${ }^{1}$
(2) $12.3 .5,12.3 .15,12.3 .29,12.3 .30$.
(3) Suppose that $M$ is an $n \times n$ matrix over C. Show that $M$ can be written in a unique way as a sum $S+N$ where:

- $S$ is diagonalizable (i.e. $S$ is conjugate to a diagonal matrix).
- $N^{n}=0$
- $S$ and $N$ commute.

Hint: For existence use Jordan decomposition. To see uniqueness, one way is to first reduce to the case when $M$ has a single eigenvalue.
(4) Let $X$ be a finite abelian group. Suppose that there exists a homomorphism $e: X \rightarrow X$ such that $e(e(x))+x=0$ for every $x \in X .{ }^{2}$ Prove that the order of $X$ is a sum of two integer squares.

Hint: think about modules over $\mathbf{Z}[i]$.
(5) (Not for handing in). Make sure you can reduce your favorite matrix of integers to diagonal form by row and column operations. The algorithm, sketched in class, is also explained in more detail in exercises 16-19 of section 12.2.

[^0]
[^0]:    ${ }^{1}$ The question of rapidly and efficiently finding a good basis for $M$ is of substantial interest in computer science and number theory. Keyword: LLL algorithm.
    ${ }^{2}$ For example: $X=\mathbf{Z} / 5 \mathbf{Z}$ and $e(x)=2 x$.

