Math 250a hw7

5.

- A $\mathbb{Z}$-module is an abelian group and vice versa. However, $\mathbb{Z}$ is not a field so we do not say $\mathbb{Z}$-vector space.
- A module is not an algebra. It may not have an identity element such as 1.
- We have to choose a *maximal* set of linearly independent elements of A over $\mathbb{R}$. Such a maximal set exists by Zorn's lemma.
- After choosing a maximal set of $\mathbb{R}$-independent elements, it is not true that $v_1, \ldots, v_{m-1}$ will generate $A \cap span_{\mathbb{R}} \{v_1, \ldots, v_{m-1}\}$ over $\mathbb{Z}$. We may *assume* it because by induction there exists some $w_1, \ldots, w_{m-1}$ that do generate, and we may replace v_i's with w_i's.
- A is additive, closed under translation up to integer multiples of its elements, but not closed under division by integers.
- The m-th coefficient of v'_m must not be zero. v'_m is chosen to make this coefficient minimal among the nonzero's.
- Base case.
- Yes. It is not important how the a_i's are bounded as long as they are, bounded.

An alternative solution formulates it as an algorithm which chooses generators iteratively. Let $B(p, r)$ denote an open ball centered at p of radius r and $|x|$ denote the Euclidean norm of $x \in \mathbb{R}^n$. If $A = \emptyset$, the statement is vacuously true. Otherwise, suppose we have chosen $m-1$ linearly independent vectors $v_1, \ldots, v_{m-1} \in A$ such that

$$A_0 = A \cap \sum_{i=1}^{m-1} \mathbb{R}v_i = \sum_{i=1}^{m-1} \mathbb{Z}v_i.$$

If $A = A_0$, then we are done. Otherwise, choose a radius r_m such that

$$S = B(0, r_m) \cap A - \sum_{i=1}^{m-1} \mathbb{R}v_i \neq \emptyset.$$

Pick a v_m such that

$$|v_m| = \min \{|v| : v \in S - \{0\}\}.$$

Minimum exists because $B(0, r_m)$ is bounded. The algorithm will halt because A is finite dimensional.

Suppose the algorithm chooses $v_1, \ldots, v_m$, then we know that $A_0 = \sum_{i=1}^{m-1} \mathbb{Z}v_i$ and $A \subset A_0 + \mathbb{R}v_i$. We claim that $A = \sum_{i=1}^{m} \mathbb{Z}v_i$. If not, up to translation there exists $rv_m \in A$ with $r \in (0, 1)$. This is a contradiction, because the algorithm would have chosen rv_m for $|rv_m| < |v_m|$.

9. (b) Do not forget the middle exactness, i.e., $\ker(S^{-1}M' \to S^{-1}M) = \operatorname{image}(S^{-1}M \to S^{-1}M'')$.

10.

(a) To see that the annihilator of some $x \in M$ is indeed an ideal, consider the A-module morphism $A \to M, a \mapsto ax$. The kernel of this morphism is the annihilator of x in A, which must be an ideal.

(b) Show that a sequence $0 \to M' \to M \to M'' \to 0$ is exact if and only if the sequence $0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0$ is exact for all primes $\mathfrak{p}$.

- If $\mathfrak{p}$ is a maximal ideal, not every element in $A - \mathfrak{p}$ is a unit. For example, (2) is a maximal ideal in $\mathbb{Z}$ and $3 \notin (2)$, but 3 is not a unit in $\mathbb{Z}$. Indeed, quotient of a ring by its maximal ideal results in a field, so they are "units" in a different ring.

One direction follows from 9(a). For the converse direction, it suffices to show that for any sequence $M' \to M \to M''$, if $M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}}$ is exact for all primes $\mathfrak{p}$, then the sequence $M' \to M \to M''$ is exact. Indeed, for injectivity or surjectivity we may let $M' = 0$ or let $M'' = 0$. We always takes annihilator of some element, possibly in a quotient module.

To see that image$(f) \subset \ker(g)$, chase the following diagram

$$\begin{array}{ccccc} M' & \longrightarrow & M & \longrightarrow & M'' \\ \downarrow & & \downarrow & & \downarrow \\ \prod_{\mathfrak{p}} M'_{\mathfrak{p}} & \longrightarrow & \prod_{\mathfrak{p}} M_{\mathfrak{p}} & \longrightarrow & \prod_{\mathfrak{p}} M''_{\mathfrak{p}} \end{array}$$

Observe that

$$(\ker(g)/\mathrm{image}(f))_{\mathfrak{p}} = \ker(g)_{\mathfrak{p}}/\mathrm{image}(f)_{\mathfrak{p}}.$$

If $\ker(g)/\mathrm{image}(f) \neq 0$, the annihilator of some $m \in \ker(g)$ with respect to image(f), i.e.

$$\ker(A \stackrel{\cdot m}{\to} \ker(g)/\mathrm{image}(f)) = \{a : am \in \mathrm{image}(f)\}$$

is a proper ideal in A, contained some maximal ideal $\mathfrak{p}$. Then $(\ker(g)/\mathrm{image}(f))_{\mathfrak{p}} \neq 0$, a contradiction.