# ALGEBRA HOMEWORK SET 7

JAMES CUMMINGS (JCUMMING@ANDREW.CMU.EDU)

Due by class time on Wednesday 3 November. Homework must be typeset and submitted by email as a PDF file.

(1) Recall that a subset $S$ of a ring $R$ is multiplicatively closed (MC) if $1 \in S$ and $S$ is closed under multiplication. Let $S \subseteq R$ be MC and define a binary relation $\sim$ on $R \times S$ as follows: $(r, s) \sim (r', s')$ iff there is $t \in S$ such that $t(rs' - r's) = 0$. Prove that:

  (a) $\sim$ is an equivalence relation.

  (b) Defining $+$ and $\times$ as in the definition of field of fractions makes the set of $\sim$-classes into a ring (which we write $RS^{-1}$). Just check the operations are well-defined, it is then clear that the ring axioms are satisfied.

  This is all routine computation. The point is that $r \mapsto r/1$ is a "universal" map such that the image of everything in $S$ is a unit, in the sense that every such map factors through it uniquely.

(2) Let $G$ be a torsion-free $\mathbb{Z}$-module (abelian group) of rank 1 and let $P$ be the set of prime numbers.

  (a) Prove that $G$ is isomorphic to a subgroup of $(\mathbb{Q}, +)$.

  Let $g \in G$ be nonzero: then for every nonzero $h \in G$ there must exist $m$ and $n$ nonzero integers such that $mg = nh$ since otherwise the rank would be greater than one.

What is more if $m'g = n'h$ for nonzero $m'$ and $n'$, then $(mn' - m'n)g = nn'h - nn'h = 0$, so $m/n = m'/n'$. It is now routine to check that setting $0 \mapsto 0$ and $h \mapsto m/n$ gives an injective HM from $G$ to $\mathbb{Q}$.

(b) Let $G \leq \mathbb{Q}$. For each nonzero $a \in G$, let $n_a : P \to \mathbb{N} \cup \{\infty\}$ be defined as follows:

$$n_a(p) = \sup\{n : a/p^n \in G\}.$$

Prove that if $a$ and $b$ are both nonzero then $n_a(p) = \infty \iff n_b(p) = \infty$, and $\{p : n_a(p) \neq n_b(p)\}$ is finite.

Let $M$ and $N$ be nonzero integers such that $Ma = Nb$. Suppose that $p$ is a prime such that $p$ does not divide $N$, and that $a/p^n \in G$. By standard number theory, since $p^n$ is coprime with $N$ there exist integers $X$ and $Y$ such that $Xp^n + YN = 1$, so $b/p^n = Xb + YNb/p^n = Xb + YMa/p^n \in G$. Similarly if $p$ does not divide $M$ and $b/p^n \in G$ then $a/p^n \in G$. It follows that for all but finitely many primes $p$ (those that divide $M$ or $N$) we have $n_a(p) = n_b(p)$.

Now let $n_a(p) = \infty$. Clearly every integer multiple of $a$ has the same property, so we may assume that $a$ is an integer. Also $ap^{-m}$ has the same property for every $m$ so we may assume that $a$ is an integer not divisible by $p$. Arguing as above for each $n$ we can find $X$ and $Y$ such that $Xa + Yp^n = 1$. Now let $b \in G$ be arbitrary, so that $b/p^n = Xa/p^n + Yb \in G$.

(3) Let $A$ be an $n \times n$ integer matrix and let $G_A$ be the subgroup of $\mathbb{Z}^n$ generated by the columns of $A$. Prove that $\mathbb{Z}^n/G_A$ is finite iff $det(A) \neq 0$, and that in this case $\mathbb{Z}^n/G_A$ has order $|det(A)|$.

Use the theorem on the structure of subgroups of free abelian groups to find a basis $b_1, \dots b_n$ of $\mathbb{Z}^n$ and nonzero numbers $c_1, \dots c_m$ such that $c_1 b_1, \dots c_m b_m$ form a basis for $G_A$. $det(A)$ is nonzero iff the columns are linearly independent over $\mathbb{Q}$ iff they are independent over $\mathbb{Z}$ iff $G_A$ has rank $n$ iff $m = n$ iff $\mathbb{Z}^n/G_A$ is finite. In this case it is clear that $\mathbb{Z}^n/G_A$ has order $c_1 \dots c_n$.

To finish we form a matrix $M$ whose $i$ column is $b_i$, and then let $C$ be diagonal with diagonal entries $c_i$ so that $MC$ has $i$ column $c_i b_i$. Expressing the columns of $I_n$ in terms of the $b_i$ we find an integer matrix $N$ such that $I = MN$. Similarly we find integer matrices $N_1$ and $N_2$ such that $A = MCN_1$ and $MC = AN_2$. Now by routine calculation $N_1$ and $N_2$ are mutually inverse integer matrices, so have determinants $\pm 1$ and the resulkt follows easily.

(4) Prove that the intersection of any nonempty chain of prime ideals is prime.

Let $C$ be such a chain. Clearly the intersection $P$ is an ideal. If $anotinP$ and $b \notin P$ then by going far enough down the chain we find $Q \in C$ such that $a, b \notin Q$. Then as $Q$ is prime $ab \notin Q$, hence $ab \notin P$.

(5) Let $R$ be a PID and let $N$ be a free $R$-module on a countably infinite set of generators (for example the set of all functions from $\mathbb{N}$ to $R$ which are zero on a cofinite set). Prove that every submodule of $N$ is free.

Let $N$ be the given free module, and note that:

(a) If we define $N_i$ to be the set of $f$ such that $f(j) = 0$ for $j > i$, then $N_i$ is a free module of rank $i+1$, and $N = \bigcup_i N_i$.
(b) If we define $\pi_i : N \to R$ by $\pi_i(f) = f(i)$ then $\pi_i$ is a HM.

For each $i$, $\pi_i[M \cap N_i]$ is an ideal of $R$, say $(a_i)$, and we may choose $m_i \in M \cap N_i$ such that $\pi_i(m_i) = a_i$. We claim that the nonzero elements $m_i$ form a basis for $M$, so we must check that they are independent and spanning. Independence is easy, because a nonzero $m_i$ has its last nonzero entry at coordinate $i$; so if $i_1 < \dots i_n$ with $m_{i_k}$ nonzero and $\sum_{k=1}^n \lambda_k m_{i_k} = 0$, then applying $\pi_{i_n}$ we have $\lambda_n a_n = 0$ so that $\lambda_n = 0$.

For spanning we do an induction on the largest $n$ such that $\pi_n(m) \neq 0$; since $m \in M \cap N_n$ we have that $\pi_n(m) = ra_n$ for some $r$, and now we can apply the induction hypothesis to $m - rm_n$.