Math 210B: Homework #1

Due on January 18, 2022

Professor Alexander Merkurjev

Nakul Khambhati

Problem 1

Proof. Let R be a finite integral domain i.e. $R \neq 0$ and it has no zero divisors. In other words, if $xy = 0$, then $x = 0$ or $y = 0$.

To prove that R is a field, we need to show that $\forall r \in R, r \neq 0 : \exists r^{-1} \in R$. Let $r \in R$ be a non-zero element of R. Consider the map of sets $m_r : R \to R$ such that $s \mapsto rs$. We show that this map is injective. Let $rs_1 = rs_2$. So $rs_1 - rs_2 = 0$ and $r(s_1 - s_2) = 0$. Since we are working within a domain and we picked $r \neq 0$, we get that $s_1 - s_2 = 0$ so $s_1 = s_2$.

We have proved that a map from R to R is injective. Since R is finite, this map is also surjective. So, $\exists r' \in R : rr' = 1$ so $r^{-1} = r'$ and r has an inverse. This shows that every non-zero element of R has an inverse, and it is a field. ☐

Problem 2

Proof. Let $A \in M_n(R)$. Then, $det(A) = 0$ is equivalent to there being an expression (the determinant formula) in terms of the coefficients of A that evaluates to 0. In others words, $det(A) = 0 \iff$ we can construct a matrix B which, when multipled with A, performs the corresponding arithmetic to return 0. Therefore, A is a zero divisor $\iff det(A) = 0$. ☐

Problem 3

Let $f : R \to S$ be a surjective ring homomorphism, $I \subset S$ an ideal. We need to show that $f^{-1}(I) \subset R$ is an ideal that contains $\ker(f)$.

Proof. From the correspondence theorem for groups, we know that $f^{-1}(I)$ is a subgroup. We need to verify $Rf^{-1}(I) \subset R$. Let $x \in f^{-1}(I), r \in R$. We need to show that $xr \in f^{-1}(I)$ i.e. $f(xr) \in I$. This is immediate since $f(xr) = f(x)f(r) \in I$ since $f(x) \in I$. Also, since $0 \in I, f^{-1}(0) = \ker(f) \subset f^{-1}(I)$.

To complete the proof, we need to show that if $I \subset R$ is an ideal containing $\ker(f)$, then $f(I) \subset S$ is an ideal. Let $s \in S$. Since f is surjective, we can write $s = f(r)$ for some $r \in R$. Let $y \in f(S)$. $f(s)(y) = f(sy)$. Since $sy \in I, f(sy) \in f(I)$. Therefore, $f(I)$ is an ideal. This yields the required bijection. ☐

Problem 4

Proof. (a) Let R be a commutative ring. Let $a, b \in Nil(R)$. So, $\exists n, n' \in \mathbb{Z} : a^n = b^{n'} = 0$. Let $m = \max\{n, n'\}$. Then $(a+b)^{2m} = a^{2m} + \ldots + a^m b^m + \ldots + b^{2m} = 0$ so $a + b \in Nil(R)$. Let $r \in R$. Then $(ra)^n = r^n a^n = 0$ so $ra \in Nil(R)$. Therefore, it it is a ring.
Assume that $\exists\ r + Nil(R) \in R/Nil(R)$ such that $(r + Nil(R))^m = r^m + Nil(R) = Nil(R)$ for some $m \in \mathbb{Z}$. This implies that $r^m \in Nil(R)$ so $r \in Nil(R)$ and $r + Nil(R) = Nil(R) = O_{R/Nil(R)}$.

(b) Let $f(t) = a_0 + a_1 t + \ldots + a_n t^n \in R[t]$. Assume that all a_i are nilpotent. Since $Nil(R[t])$ is a ring, $a_i \in Nil(R[t]) \Rightarrow a_i t_i \in Nil(R[t])$ and $a, b \in Nil(R[t]) \Rightarrow a + b \in Nil(R[t])$. Therefore, $f(t) \in Nil(R)$.
Assume that $f(t)$ is nilpotent i.e. $(a_0 + a_1 t + \cdots + a_n t^n)^m = 0$ for some $m \in \mathbb{Z}$. In particular, $a_0^m = 0$ so a_0 is nilpotent. By closure of a ring, $t(a_1 + a_2 t + \cdots + a_n t^{n-1})$ is nilpotent. So a_1 is nilpotent as before. We can proceed by induction to prove that all a_i must be nilpotent.

☐

Problem 4 continued on next page. . .

Problem 5

Proof. (a) Let $a \in R$ be nilpotent i.e. $\exists \in \mathbb{N}$ such $a^n = 0$. We want to find some $b \in R$ such that $(1+a)b = 1$. Recall that $(1+a)(1-a+\cdots+(-1)^{n-1}a^{n-1}) = 1+(-1)^n a^n = 1$. Therefore, $1+a \in R^\times$

(b) Assume that a_0 is invertible and $a_i, i \geq 1$ are nilpotent.

Lemma 1. *Let $u \in R^\times, a \in Nil(R)$. Then, $u + a \in R^\times$.*

Proof of lemma. We write $u + a = u(1 + u^{-1}a)$. Since $u^{-1}a$ is nilpotent, $1 + u^{-1}a$ is invertible by (a) so $u + a$ is invertible. □

Appying this lemma to $f(t) = a_0 + a_1 t + \cdots + a_n t^n$, we are given that a_0 is invertible and it is easy to see that $a_1 t + \cdots + a_n t^n$ is nilpotent. Therefore, $f(t)$ is invertible.
Conversely, assume that $f(t)$ is invertible. Then $\exists g(t) = b_0 + b_1 t + \cdots + b_m t^m$ such that $f(t)g(t) = 1$. Upon expanding and comparing terms, we see that $a_0 b_0 = 1$ so a_0 is invertible. Also, $a_n b_m = 0$ and $a_{n-1} b_m + a_n b_{m-1} = 0$. Multiplying across by a_n, we get $a_n^2 b_{m-1} = 0$. We can keep repeating this step till it cascades down to $a_n^m b_0 = 0$. Since b_0 is a unit, $a_n \in Nil(R)$. By induction, we get that all $a_i \in Nil(R)$.

□

Problem 6

Proof. Let $r \in R$ and $f : \mathbb{Z}[t] \to R$ be a ring homomorphism such that $f(t) = r$. Let $p(t) \in \mathbb{Z}[t], p(t) = a_0 + a_1 t + \cdots + a_n t^n, a_i \in \mathbb{Z}$. Then, $f(p) = f(a_0) + f(a_1)r + \cdots f(a_n)r^n$ which is unique since $f(m)$ is uniquely determined for $m \in \mathbb{Z}$. We know that $Im(f) \subset R$ is a subring that contains r. To prove that it is the smallest such subring, let $S \subset R$ be a subring such that $r \in S$. By closure under a ring, $r^i \in S, a_i r_i \in S$ for $a_i \in \mathbb{Z}$ and $r^i + r^j \in S$. Therefore, $Im(f) \in S$. □

Problem 7

Proof. Let R be a domain such that $R[t]$ is a PID. Recall that $R \cong R[t]/(t)$. Since R is a domain, so $(t) \subset R[t]$ is a prime ideal. Now we show that every prime ideal P in a PID is also maximal.

Let P be a prime ideal and $P \subset I \subset R$. Since R is a PID, we write $P = (a), I = (b)$. Clearly $a \in (b)$ therefore we can write $a = bc$ for some $c \in R$. Since P is prime, this means that $b \in P$ or $c \in P$. If $b \in P$ then $I = (b) \subset P$ and $I = P$. If $c \in P$ we can write $c = ad$ for $c \in R$. Then, $a = bad$ i.e. $bd = 1$ so $b \in R^\times$. Then, $I = R$. We have shown that $P \subset I \subset R$ implies that $I = P$ or $I = R$. Therefore, P is maximal.

We are almost done. From above, (t) is maximal. Therefore, $R \cong R[t]/(t)$ is a field. □

Problem 8

Proof. Let R be a non-zero commutative ring. By Zorn's lemma, it has a prime ideal P. Now consider $P \in R[t]$. $xy \in P \Rightarrow x \in P \vee y \in P$ so P is prime in $R[t]$ as well. It then follows that we can construct infinitely many more prime ideals $(Pt), (Pt^2), (Pt^3), \ldots$ □

Problem 9

We define $Rad(R) = \bigcap_{M \subset I} M$.

Proof. $\Leftarrow$ Assume that $\forall y \in R, 1 - xy \in R^\times$. Also assume, in search of a contradiction, that $x \notin Rad(R)$ i.e. $\exists M : x \notin M$. Then, $(x) + M = R$. In particular, $\exists y \in R, m \in M : xy + m = 1$. We can write $m = 1 - xy$. By hypothesis, this is invertible. But then M contains an invertible element so $M = R$ which is a contradiction. So, $x \in Rad(R)$.
$\Rightarrow$ Assume that $x \in Rad(R)$ and assume, in search of contradiction, that $\exists y \in R : 1 - xy$ is not invertible. Any element that is not invertible is contained in some maximal ideal so $1 - xy \in M$ for some M. Write $m = 1 - xy$. But since $x \in Rad(R)$ by assumption, $x \in M$ so $xy \in M$. Then $m + xy = 1 \in M$ and $M = R$, a contradiction. So $\forall y \in R, 1 - xy \in R^\times$. $\square$

Problem 10

Proof. Let X be a set, R be a commutative ring. Recall that a ring homomorphism $h : \mathbb{Z}[X] \to R$ is uniquely determined by a set map $f : X \to R$. In other words, we have a bijection $Hom_{CRings}(\mathbb{Z}(X), R \cong Maps(X, R)$. Let F be the forgetful functor and G be the functor that takes any set $X \mapsto \mathbb{Z}[X]$. Then, we can rewrite the above bijection as $Hom_{CRings}(G(X), R \cong Maps(X, F(R)))$. Clearly, G is left-adjoint to F. $\square$