Homework 7

Kevin Guillen

MATH 200 — Algebra I — Fall 2021

May I please have my proof for problem 10.3 graded, thank you.

Problem 7.2 (a) Let G be a cyclic group of prime order p. Show that $\mathrm{Aut}(G)$ has order $p-1$.

(b) Let G be a group of order pq with primes $p < q$ such that $p \nmid q-1$. Show that G is cyclic

(a) *Proof.* We know that G is cyclic and therefore $G = \{g, g^2, \ldots, g^p = e\} =< g >$. In other words g is a generator of G. We know if we have an automorphism f, that $f(g)$ has to map to a generator of G. Note thoug that all elements of G have order p except e, meaning all elements of G are generators except e. Therefore there are only $p-1$ choices, meaning there are only $p-1$ autmorphisms for G. □

(b) *Proof.* Let $H \in \mathrm{Syl}_p(G)$ and $H' \in \mathrm{Syl}_q(G)$. We know the number of Sylow $p-$subgroups of G is $1+np$, and has to divde pq. We know though that $1+np$ cannot divide p and therefore must divide q. Recall though we are given that q is another prime, therefore $1+np = 1, q$. But consider the following,

$$\begin{aligned} 1+np &= q \\ np &= q-1 \\ \to p &\mid q-1 \end{aligned}$$

which can't be because we were given that $p \nmid q-1$. Therfore $1+np = 1$, which means $|\mathrm{Syl}_p(G)| = 1$, and by the same reasoning $|\mathrm{Syl}_q(G)| = 1$. From here we know then that $H \cap H' = e$, and therefore when considring the union of these 2 subgroups we know there will be $p+q-1$ elements. Note though that

$$p+q-1 < 2q \leqslant pq$$

which means there exists and element $e \neq a \in G$, that is neither in H or H', and $o(a) = pq$. Which means that G is indeed cyclic. □

Problem 9.2 (a) Let R be a finite integral domain. Show that R is a field.

(b) Let R be a division ring. Show that $Z(R)$ is a field.

(a) *Proof.* Given that R is a finite integral domain, all that is missing to show it is a field is that every element has a multiplicative inverse. To show this let us consider a non-zero element $a \in R$. We want to show this element has an inverse by showing there is some element $r \in R$ such that $ar = 1_R$. We know because R is finite we can consider all its elements as $\{r_1, r_2, \ldots, r_n\}$ for some $n \in \mathbb{N}$.

Next we know the set $\{ar_i | r_i \in R, i = 1, \ldots, n\}$ must be the same size as R. This is because for two elements $r_i, r_j \in R$, $i \neq j$, we would have $ar_i = ar_j$, but we are in an integral domain so this implies $r_i = r_j$ which would be a contradiction. Therefore there must be some $i \in \{1, \ldots, n\}$ such that $ar_i = 1_R$. Meaning for any nonzero element $a \in R$, it has a multiplicative inverse in R, making R a field. □

(b) *Proof.* Given that R is a division ring, we know that every element in $Z(R)$ commutes with every element in R. Consider an element $x \in Z(R)$, we want to show that $x^{-1} \in Z(R)$. Let $r \in R$, we know that $xr = rx$ and that $(xr) \in R$, meaning there exists $(xr)^{-1}$ because R is a division ring. We see though,

$$
\begin{aligned}
(xr)^{-1} &= (rx)^{-1} \\
r^{-1}x^{-1} &= x^{-1}r^{-1}.
\end{aligned}
$$

Notice though that r was arbitrary in R, and therefore x^{-1} commutes with every element in R, meaing $x^{-1} \in Z(R)$. Therefore $Z(R)$ is indeed a field. □

Problem 10.2 (a) Show that $\{0\}$ and D are the only ideals of D.

(b) Let R be a non-trivial ring and let $f : D \mapsto R$ be a ring homomorphism. Show that f is injective.

(a) *Proof.* Let I be an ideal of D such that $I \neq \{0\}$. This means there is some element $a \in I$, and because $I \subseteq D$, $a \in D$. Now let b be any element in D. We know D is closed under multiplication so $ba^{-1} \in D$. We also know that $(ba^{-1})a \in I$, because $a \in I$. Observe though,

$$
\begin{aligned}
(ba^{-1})a &\in I \\
b(a^{-1}a) &\in I \\
b1_D &\in I \\
b &\in I.
\end{aligned}
$$

We said b to be any element in D, thus if I as any non-zero element in it, $D \subseteq I$.Wwe also had though that $I \subseteq D$, therfore $I = D$ if $I \neq \{0\}$, given that D is a division ring. □

(b) *Proof.* In class we defined ring homomorphimsms to respect multiplicative identites between rings. This is key because consider $a \in ker(f)$ and assume $a \neq 0$. That means $f(a) = 0$, we also know $\exists a^{-1} \in D$, so consider the following,

$$
\begin{aligned}
f(1) &= f(aa^{-1}) \\
&= f(a)f(a^{-1}) \\
&= 0f(a^{-1})
\end{aligned}
$$

$$= 0.$$

This can't be though since a proper ring homomorphimsm as we defined in class we must have $f(1) = 1$. Therefore the kernel of f must be trivial which means, f is indeed injective. $\square$

Problem 10.3 (a) Let F be a field. Show that the characteristic of F is either a prime number or 0.

(b) Let p be a prime and let R be a ring with p elements. Show that $R \cong \mathbb{Z}/p\mathbb{Z}$.

(a) *Proof.* If $\mathrm{char}(F) = 0$ then we are done. We know that $\mathrm{char}(F) \neq 1$ because that would imply $1 = 0$ which means F is not a field. Now if $\mathrm{char}(F) = n$, assume n to be composite, meaning there exists 2 natural numbers, k, l, where $1 < k, l < n$ such that $n = kl$. Consider the following,

$$\begin{aligned}(k \cdot 1)(l \cdot 1) &= kl \cdot 1 \\ &= n \cdot 1 \\ &= 0.\end{aligned}$$

Recall though a field is an integral domain meaning there are no zero divisors, therefore either $(k \cdot 1) = 0$ or $(l \cdot 1) = 0$. Also recall though n is supposed to be the smallest non-negative integer such that $n \cdot 1 = 0$. So if either of the two cases were to be true it would contradict the minimality of n. Therefore if $\mathrm{char}(F) = n$, n has to be a prime number. All together we have show that $\mathrm{char}(F) = 0$ or $\mathrm{char}(F) = p$ where p is a prime. $\square$

(b) *Proof.* Consider the unique homomorphism from the ring of integers to any ring R,

$$\begin{aligned}f : \mathbb{Z} &\to R \\ z &\mapsto z1_R.\end{aligned}$$

We already know this is indeed a ring homomorphism. So by definition we know the image of f will be mapped to a subring of R. The only two options is $\{0\}$ and R itself since R has p elements and therefore the order of the subring must divide p. We know it cant be $\{0\}$ though since ring homomorphism respect multiplicative identities, meaning $f(1_\mathbb{Z}) = 1_R$. Therfore f is surjective meaning $\mathrm{im}(f) = R$.

Now according to the fundamental theorem of homomorphisms $\mathbb{Z}/\ker(f) \cong \mathrm{im}(f)$. We already know $\mathrm{im}(f) = R$. We also know that the only subrings of $\mathbb{Z}$ are of the form $n\mathbb{Z}$, meaning $\ker(f) = n\mathbb{Z}$ for some $n \in \mathbb{N}_0$. All this together gives us $\mathbb{Z}/n\mathbb{Z} \cong R$. Isomorphisms though are 1-1 meaning the two rings must be of the same order, R has p elements, so $\mathbb{Z}/n\mathbb{Z}$ must have p, elements, but this can only be true if $n = p$. Therefore $\mathbb{Z}/p\mathbb{Z} \cong R$, as desired.

$\square$

Problem 10.4 Let R be a ring. An element $r \in R$ is called *nilpotent* if there exists $n \in \mathbb{N}$ such that $r^n = 0$.

(a) Show that if $r \in R$ is nilpotent then $1 - r$ is a unit of R.

(b) Show that if R is commutative then the nilpotent elements of R form an ideal N of R.

(c) Show that if R is commutative and N is the ideal of nilpotent elements then 0 is the only nilpotent element of R/N

(a) *Proof.* Given that r is nilpotent, consider the following,

$$1 = (1 - 0) = (1 - r^n) = (1 - r)(1 + r + r^2 + \cdots + r^{n-1}).$$

This means that the inverse of $1 - r$ is simply $(1 + r + \cdots + r^n)$ □

(b) *Proof.* Let N be the set of all nilpotent elements of R. It is clear that 0 is in this set because $0^1 = 0$.

Let $x, y \in N$, we want to now show that $(x - y) \in N$. We will use what we know about binomial expansion to show there exists and $n \in \mathbb{N}$ to show that $(x - y)^n = 0$. We already know there exists a n_1 and n_2 such that $x^{n_1} = 0$ and $y^{n_2} = 0$. That means for all $n_1' > n_1$ and $n_2' > n_2$ we have $x^{n_1'} = 0$ and $y^{n_2'} = 0$.

That means if we let $b = \max(n_1, n_2)$, $x^b = 0 = y^b$.

This is important to us because, ignoring the coefficents for a moment, we know that $(x-y)^n$ expanded is,

$$ax^n y^0 + bx^{n-1}y^1 + \cdots + zx^0 y^n.$$

This means we can find a n sufficently large enough such that for each term in the expansion $x^p y^q$ either p or q will be greater than b resulting in the term being 0. It's obvious in this case $n = 2b$, this way for every term $x^p y^q$ either $p \geqslant b$ or $q \geqslant b$. Meaning every term will then be 0, implying $(x - y)^n = 0$, therefore $(x - y) \in N$

Finally we want to show that for any $a \in R$ and for any $x \in N$ that $ax \in N$. We know there exists some $n \in \mathbb{N}$ such that $x^n = 0$. So consider the following,

$$\begin{aligned}(ax)^n &= a^n x^n \\ &= a^n 0 \\ &= 0\end{aligned}$$

therfore $(ax) \in N$. Altogether we have that N is indeed an ideal of R, given that R is commutative. □

(c) *Proof.* Let $r \in R$, and let us denote $r + N$ as x. If x is nilpotent that means there is a $n \in \mathbb{N}$ such that,

$$x^n = (r + N)^n = r^n + N = 0 + N = N$$

Which means that $r^n \in N$, and therfore exists an $k \in \mathbb{N}$ such that $(r^n)^k = 0$. This means r is a nilpotent element of R, meaning $x = N$, which is the zero of R/N. □