Homework 6

Hussein Zamzami
Math-321
Dr. David Carchedi
G00737304

December 8, 2015

1 Herstein Section 4.1, problem 14

Show that the only quaternions commuting with i are of the form $\alpha + \beta i$.

Proof. First, we must show that the quaternions of the form $\alpha + \beta i$ commute with i. Take $i(\alpha+\beta i) = (\alpha i-\beta)$, by distributive law. Similarly, take $(\alpha+\beta i)i = (\alpha i - \beta)$, this proves that the quaternions of the form $(\alpha + \beta i)$ commute. Now we must show that any other quaternion does not commute with i. Quaternions not of the form $(\alpha + \beta i)$ will feature a j or a k as part of the quaternion. Let a, be a quaternion not of the highlighted form, then ia will feature either the product ij and/or ik, but ai will feature the product ji and/or ki. Therefore, for $ia = ai$, we must have $ij = ji$ and $ki = ik$, but the quaternions do not form a commutative ring and i, j, k do not commute, therefore $ai \neq ia$, therefore any quaternion not of the form $(\alpha + \beta i)$ does not commute with i. □

2 Herstein Section 4.1, problem 15

Find the quaternions that commute with both i and j.
The only quaternions commuting with i are of the form $(\alpha + \beta i)$, therefore by the same logic as the above problem, the only quaternions that commute with j are of the form $(\alpha + cj)$, therefore our quaternion, q has to be both of the form $(\alpha + \beta i)$ and $(\alpha + cj)$. Set $\beta = c = 0$, so that q is simply (α). Then, clearly $ai = ia$, as multiplication by a real number is commutative, and $aj = ja$.

3 Herstein Section 4.1, problem 19

Show that there is an infinite amount of solutions to $x^2 = -1$ in the quaternions.

Proof. Let $q = \beta i + cj + dk$, with $\beta, c, d \in \mathbb{R}$, specifically in the interval $[-1, 1]$ and $\beta^2 + c^2 + d^2 = 1$, then $q^2 = -\beta^2 - c^2 - d^2 = -1(\beta^2 + c^2 + d^2) = -1$ and

since there are an infinite amount of real numbers, there are an infinite mount of solutions to the equation $-1(\beta^2 + c^2 + d^2)$ is a solution. $\square$

4 Herstein Section 4.1, problem 36

if $F = \mathbb{C}$, the complex numbers, show that $H(\mathbb{C})$ is not a division ring.

Proof. $H(\mathbb{C})$ is the ring of quaternions over the complexes, i.e. a ring whose elements are of the form $(\alpha_0 + \beta_0 i) + (\alpha_1 + \beta_1 i)i + (\alpha_2 + \beta_2 i)j + (\alpha_3 + \beta_3 i)k = (\alpha_0 + \beta_0 i) + (\alpha_1 i - \beta_1) + (\alpha_2 j + \beta_2 k) + (\alpha_3 k - \beta_3 j)$. We wish to show that there is no inverse of this quaternion q, such that $qq^{-1} = q^{-1}q = 1$ let q^{-1} be the normal quaternion inverse, then $q^{-1} = \frac{(\alpha_0+\beta_0 i)-(\alpha_1 i-\beta_1)-(\alpha_2 j+\beta_2 k)-(\alpha_3 k-\beta_3 j)}{(\alpha_0+\beta_0 i)^2+(\alpha_1-\beta_1 i)^2+(\alpha_3+\beta_3 i)^2+(\alpha_3+\beta_3 i)^2}$. We will show that this does not in fact constitute an inverse, take $qq^{-1} = ((\alpha_0 + \beta_0 i) + (\alpha_1 i - \beta_1) + (\alpha_2 j + \beta_2 k) + (\alpha_3 k - \beta_3 j))\frac{(\alpha_0+\beta_0 i)-(\alpha_1 i-\beta_1)-(\alpha_2 j+\beta_2 k)-(\alpha_3 k-\beta_3 j)}{(\alpha_0+\beta_0 i)^2+(\alpha_1-\beta_1 i)^2+(\alpha_2+\beta_2 i)^2+(\alpha_3+\beta_3 i)^2}$ For this product to be 1, the numerator will have to equal the denominator and for that to occur, all the imaginary units in the numerator will have to be either i^2, j^2, k^2, or ijk. One of the products in the numerator, however, is $(\alpha_2 j + \beta_2 k)(\alpha_3 k + \beta_3 j) = (-\alpha_2\beta_2 + \alpha_2\alpha_3 jk + \beta_2\beta_3 jk - \beta_2\alpha_3) = (-\alpha_2\beta_3 + \alpha_2\alpha_3 jk + \beta_2\beta_3 kj - \beta_2\alpha_3) = (-\alpha_2\beta_3 + \alpha_2\alpha_3 i - \beta_2\beta_3 i - \beta_2\alpha_3)$ This is clearly not an element in the denominator, however, so the numerator and denominator do not cancel out, yielding 1. Hence, the inverse of a quaternion in $\mathbb{H}$ does not hold in $H(\mathbb{C})$, therefore there are no inverses in $H(\mathbb{C})$, hence it is not a division ring. $\square$

5 Herstein Section 4.3, problem 4

If I, J are ideals of R, define $I + J = \{i + j | i \in I, j \in J\}$, show that $I + J$ is an idea of R.

Proof. Let $L = I + J$, for L to be an ideal of R, we need that $L \leq (R, +)$ and that $\forall r \in R, a \in L, ra \in L, ar \in L$. The first follows from the definition of L, as both I and J are additive subgroups of R. For the second, take $r \in R$ and $a \in L$, then $ra = r(i + j), i \in I, j \in J$, this is equal to $ri + rj$ and we know, since I, J are ideals, that $ri \in I, rj \in J$, therefore $ri + rj \in L$, as it satisfies the definition of an element in L. Following a similar logic, it follows that $ar \in L$ for $r \in R, a \in L$. Therefore, $L = I + J$ is an ideal. $\square$

6 Herstein Section 4.3, problem 5

If I is an ideal of R and $A \leq R$, show that $I \cap A$ is an ideal of R.

Proof. Let $L = I \cap A$, by definition of intersection, any element $a \in L$ is in I, hence $L \leq I$, therefore it is clear that L is an additive subgroup of R, all that remains is to show that $ra \in L$ and $ar \in L$, for $a \in L, r \in A$. Take ra,

since $L \leq I$, $a \in I$ and, clearly, $ra \in I$. All that remains to be shown is that $ra \in A$, where A is any subring of R. Since A is a subring, it is closed under multiplication, i.e. $\forall x, y \in A, xy, yx \in A$ and since $r \in A$ and $a \in A$, therefore $ra \in A$, hence $ra \in A \cap X$. Following similar logic, it follows that $ar \in A \cap X$, therefore $L = A \cap X$ is an ideal.. $\square$

7 Herstein Section 4.3, problem 6

If I, J are ideals of R, show that $I \cap J$ is an ideal of R

Proof. Let $L = I \cap J$, then L is a subgroup of both I and J, as all the elements in L are in both I and J, therefore L is an additive subgroup of R. Now, take $r \in R$ and $a \in L$. ra is clearly an element of both I and J as $a \in I \wedge J$ and I, J are ideals of R, therefore $ra \in I \wedge J \implies ra \in L$, using similar logic, it follows that $ar \in L$, therefore $L = I \cap J$ is an ideal of R. $\square$

8 Prove Theorem 4.3.4 in Herstein

Prove the Correspondence Theorem: Let the mapping $\phi : R \longrightarrow R'$ be a surjective homomorphism with kernel K. if I' is an ideal of R', let $I = \{a \in R | \phi(a) \in I'\}$. Then I is an ideal of R, $I \supset K$ and $I/K \simeq I'$. This sets up a bijection between all ideals of R' and those ideals of R containing K.

Proof. First, we must check that I is an ideal of R. Take $r \in R$ and $a \in I$, then $ra \in I$ if $\phi(ra) \in I'$. Take $\phi(ra) = \phi(r)\phi(a)$ and $\phi(a) \in I'$, while $\phi(r) \in R'$, therefore, since I' is an ideal of R', $\phi(r)\phi(a) = \phi(ra) \in I'$, hence $ra \in I$, a similar reasoning is used to show that $ar \in I$, therefore I is an ideal of R. Now we must show that $K \subset I$. Assume an element $k \in K$, then $\phi(k) = 0$. Since I' is an ideal, it is also an additive subgroup, therefore $\phi(k) \in I'$, and hence $k \in I \forall k \in K$. It is clear that the converse is not true, as $\phi(b) \neq 0$ is a valid element of I', making b a valid element of I, but obviously, $b \notin K$. To show that $I/K \simeq I'$ is trivial, as you can define $\psi : I \longrightarrow I'$ to be simply $\psi : a \mapsto \phi(a)$, where ϕ is the homomorphism defined above. This is clearly surjective, as the elements in I are defined to be the elements in R, that get sent to elements in I'.The kernel here is the kernel of ϕ, which is K. Therefore, by the first homomorphism theorem, $I/K \simeq I'$. $\square$

9 Prove Theorem 4.3.5 in Herstein

Prove the second homomorphism theorem: Let A be a subring of a ring R and I an ideal. Then $A + I = \{a + i | a \in A, i \in I\}$ is a subring of R, I is an ideal of $A + I$, and $(A + I)/I \simeq A/(A \cap I)$

Proof. First we will prove that $A + I$ is, indeed a subring of R. To do so, we will need to show that it is closed under addition, multiplication, and additive

inverses. Take $(a_0 + i_0) + (a_1 + i_1) = (a_0 + a_1) + (i_0 + i_1)$, since addition is commutative and clearly $(a_0+a_1) \in A$ and $(i_0+i_1) \in I$, as A is a subring and I is an ideal, therefore $(a_0+i_0)+(a_1+i_1) \in A+I$, similarly, take $(a_0+i_0)*(a_1+i_1) = (a_0a_1+a_0i_1+a_1i_0+i_0i_1)$, where $a_0a_1 \in A$ and $a_0i_1, a_1i_0, i_0i_1 \in I$, as I is an ideal, therefore $a_0i_1+a_1i_0+i_0i_1 \in I$ and $(a_0a_1)+(a_0i_1+a_1i_0+i_0i_1) \in A+I$. Finally, we must show that $A + I$ is closed under additive inverses. Take $-(a_0 + i_0) = -a_0 + -i_0$, this is an element of $A + I$ if $-a_0 \in A$ and $-i_0 \in I$, but this is clear since A is a subring and is closed under additive inverses and I is an additive subgroup, closed under inverses. Therefore $(-a_0+-i_0) \in A+I$. Hence $A + I$ is a subring of R. Secondly, we will show that I is an ideal of $A + I$. Take $a + i \in A + I$ and $i_1 \in I$, we wish to show that $(a + i)i_1 \in I$. Now, $(a+i)i_1 = ai_1 + ii_1$ since I is an ideal of R, we know that $ai_1, ii_1 \in I$ and since I is an additive subgroup $ai_1 + ii_1$ must be in I and it is clear that $i_1(a + i)$ is also in I following similar reasoning, therefore I is an ideal of $A + I$. Finally, it suffices to show, using the first homomorphism theorem, that there exists a surjective homomorphism $\phi : (A + I) \longrightarrow A/(A \cap I)$ with kernel I. Let ϕ be the map $\phi : a + i \mapsto a$. It is easy to check that the kernel here is I as for any i, we have $\phi(i) = \phi(0 + i) = 0$, which is the zero element and for any element $a + i$, $\phi(a + i) = 0 \implies a = 0$, therefore $(a + i) = (0 + i) \in I$. Furthermore, it is clear that the homomorphism is surjective, as any element $a \in A$ has an analogue $a+i \in A+I$, hence $(A+I)/I \simeq A/(A\cap I)$, by the first homomorphism theorem. □

10 Prove Theorem 4.3.6 in Herstein

Prove the Third Homomorphism Theorem: Let $\phi : R \longrightarrow R'$ be a surjective homomorphism with kernel K. If I' is an ideal of R' and $I = \{a \in R | \phi(a) \in I'\}$, then $R/I \simeq R'/I'$.

Proof. For $R/I \simeq R'/I'$, there must be a surjective homomorphism $\phi : R \longrightarrow R'/I'$ with kernel I. Let ϕ be the above defined homomorphism, only now mapped to R'/I', clearly it retains its surjectivity, as it is now mapped to a smaller ring. Let a be an element of I, then $\phi(a) \in I'$, by the definition of I, which means that $\phi(a) = 0$ in R'/I'. Furthermore, for an element b, for $\phi(b)$ to equal 0, then $\phi(b)$ would have to be in I' and any such element is in I, therefore the kernel of $\phi : R \longrightarrow R'/I'$ is I and by the first homomorphism theorem, this implies that $R/I \simeq R'/I'$. □

11

Let $\phi : R \longrightarrow S$ be a ring homomorphism and I an ideal. Prove the following:
1) $\phi^{-1}(I) := \{r \in R | \phi(r) \in I\}$ is an ideal of R.

Proof. Let $I' = \phi^{-1}(I)$. For I' to be an ideal, then for any $r \in R$, $a \in I'$, $ra, ar \in I'$, which is only true if $\phi(ra), \phi(ar) \in I$. Take $\phi(ra) = \phi(r)\phi(a)$ with

$\phi(a) \in I$ and $\phi(r) \in S$, therefore $\phi(r)\phi(a) \in I$, hence we have that $\phi(ra) \in I$ and $\phi(ar) \in I$, using similar reasoning. Therefore, $ra \in I'$, for $r \in R$ and it follows, using similar argumentation that $ar \in I'$, therefore I' is an ideal of R. □

2) If I is prime, so is $\phi^{-1}(I)$

Proof. Let $I' = \phi^{-1}(I)$, for I' to be prime, we have to have that if $ab \in I$, for $a, b \in R$, then either $a \in I$ or $b \in I$. Assume $ab \in I'$, then $\phi(ab) \in I \implies \phi(a)\phi(b) \in I$. Now, since I is prime, this implies that one and only one of $\phi(a), \phi(b)$ is in I, therefore, one and only one of a, b are in I'. Hence, I' is prime. □

12

Prove that a commutative ring R is a field iff any ring homomorphism $\phi : R \longrightarrow B$ with B a non-zero commutative ring is injective.

Proof. ($\Leftarrow$) Assume $\phi : R \longrightarrow B$ with B a non-zero commutative ring is injective, then $Ker(\phi)$ is trivial, i.e. $Ker(\phi) = \{0\}$. Since R is already a commutative ring, all that remains to be shown is that this implies that R is also a division ring, i.e. R is closed under multiplicative inverses. Since ϕ is injective, we have that if $\phi(a) = \phi(b)$, then $a = b$ and $a - b = 0$. Assume a is a non-zero element of R with no inverse, then $ab = ca \implies b = c$, but if $\phi(ab) = \phi(ac)$, then $ab = ac$ and $ab - ac = 0$, since ϕ is injective, therefore $a(b - c) = 0 \implies a = 0 \vee b = c$, both of these contradict the assumption that a is a non-zero element that has no inverse. Therefore, every element has an inverse, hence R is a field.
($\Rightarrow$) Assume R is a field, then $ab = ac \implies b = c, \forall a, b, c \in R$. Assume ϕ is a non-injective homomorphism. Assume a is a non-zero element of $ker(\phi)$, then $\phi(a) = 0$, $\phi(aa^{-1}) = 0 \implies \phi(1) = 0$, this contradicts the assumption that ϕ is a homomorphism, as $\phi(1)$ must equal 1, for ϕ to be a homomorphism. Therefore, $Ker(\phi) = \{0\}$ and, hence, ϕ is an injective homomorphism. □

13

A commutative ring R is called local if it has precisely one maximal ideal. Prove that if $\mathfrak{M}$ is an ideal of R, such that every element $R - \mathfrak{M}$ (complement of $\mathfrak{M}$ in R) is a unit, then $\mathfrak{M}$ is a maximal ideal and R is a local ring.

Proof. Assume $\mathfrak{M}$ an ideal and $R - \mathfrak{M}$ is a field. Assume $\mathfrak{M}$ is not maximal, therefore $\exists I \supset \mathfrak{M}$, where I is an ideal of R, and $\exists a \in I, \notin \mathfrak{M}$ this implies that $a + \mathfrak{M} \neq 0 (\in \mathfrak{M})$. We wish to show that this implies that I is in fact R itself, that the identity in R is also in I, to show this, take for some $b \in R$, $(a + \mathfrak{M})(b + \mathfrak{M}) = (ab + \mathfrak{M}) = (1 + \mathfrak{M}) \implies ab - 1 \in \mathfrak{M}$. Let $m \in \mathfrak{M} = ab - 1$, then we have that $ab - m = 1$, therefore $1 \in I$ and we know that $ab \in I$, since I is an ideal, and $m \in I$, since $m \in \mathfrak{M} \subset I$, therefore $I = R$, therefore if I, such

that $\mathfrak{M}$ is a proper subset of I, then I. Hence, $\mathfrak{M}$ is a maximal ideal, as there are no ideals between $\mathfrak{M}$ and R. Now we must show that if L is a maximal ideal of R, then $L = \mathfrak{M}$. Assume $L \neq \mathfrak{M}$, then L is still an ideal of $R - \mathfrak{M}$, the only ideals of $R - \mathfrak{M}$ are the zero ideal and $R - \mathfrak{M}$ itself, however, since it is a field. This implies that $R - \mathfrak{M}$ is a maximal ideal of R. To demonstrate that $R - \mathfrak{M}$ is not an ideal of R, take $m \in \mathfrak{M}$ and $r \in R - \mathfrak{M}$. Clearly, $m \in R$, therefore rm must be in $R - \mathfrak{M}$. $rm \in \mathfrak{M}$, however, so it cannot be in $R - \mathfrak{M}$, therefore for any $m \in R$, $r \in R - \mathfrak{M}$, $rm \notin R - \mathfrak{M}$, hence $R - \mathfrak{M}$ is not an ideal of R. If L is the zero ideal than it is not maximal, as then $L \subset \mathfrak{M}$, therefore if L is a maximal ideal, then $L = \mathfrak{M}$. $\square$