MATH 3032: Abstract Algebra

Assignment 2

Solutions

1. **Let $\mathbb{Z}[\sqrt{-5}]$ denote the unital subring of $\mathbb{C}$ consisting of those complex numbers $a+b\mathbf{i}$ such that $a \in \mathbb{Z}$ and $b \in \sqrt{5}\mathbb{Z}$. Said differently, $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5}$ s.t. $a, b \in \mathbb{Z}\}$.**

   (a) **Describe the ideal $(2) \subset \mathbb{Z}[\sqrt{-5}]$: for which integers a, b is $a + b\sqrt{-5} \in (2)$?**
   $a + b\sqrt{-5} \in (2)$ if and only if a and b are both even.

   (b) **Describe the ideal $(1 + \sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$: for which integers a, b is $a + b\sqrt{-5} \in (1 + \sqrt{-5})$?**
   By definition, $(1 + \sqrt{-5})$ consists of the complex numbers of the form $(1 + \sqrt{-5})(m + n\sqrt{-5}) = (m-5n)+(m+n)\sqrt{-5}$ for integers m, n. In other words, $a+b\sqrt{-5} \in (1+\sqrt{-5})$ if and only if the numbers m, n defined by
   $$m = \frac{a + 5b}{6}, \qquad n = \frac{b - a}{6}$$
   are integers. Note that $n = b - m$ and b is definitionally an integer, so m is an integer if and only if n is, and they are both integers if and only if $a \equiv b \mod 6$.

   Recall that the *norm* of a complex number z is $N(z) = z\bar{z}$, i.e. $N(a + b\mathbf{i}) = a^2 + b^2$. Recall also that that $N(zw) = N(z)N(w)$ for all complex numbers z, w.

   (c) **Show $N(z) \in \mathbb{Z}$ whenever $z \in \mathbb{Z}[\sqrt{-5}]$. Conclude that if $N(w) = n$, then $N(z) \in n\mathbb{Z}$ for all elements of the principle ideal $(w) \subset \mathbb{Z}[\sqrt{-5}]$. In particular, conclude that $N(z) \in 4\mathbb{Z}$ whenever $z \in (2)$ and that $N(z) \in 6\mathbb{Z}$ whenever $z \in (1 + \sqrt{-5})$.**
   $N(a+b\sqrt{-5}) = a^2 + 5b^2$ is obviously an integer whenever a, b are. The rest follows from multiplicativity of $N(-)$.

   (d) **Show that if $z, w \in \mathbb{Z}[\sqrt{-5}]$, then $N(z+w) = N(z)+N(w) \mod 2$. Conclude that the ideal $(2, 1 + \sqrt{-5}) = (2) + (1 + \sqrt{-5})$ is not the whole ring $\mathbb{Z}[\sqrt{-5}]$.**
   For the first statement, note that $N(a + b\sqrt{-5}) = a^2 + 5b^2 \equiv a + b \mod 2$. For the second statement, note that $N(1) = 1$ is odd.

   (e) **Show that there does not exist an element $z \in \mathbb{Z}[\sqrt{-5}]$ such that $N(z) = 2$.**
   Suppose that $2 = N(a + b\sqrt{-5}) = a^2 + 5b^2$. If $b \neq 0$ is an integer, then $b^2 \geq 1$, so $a^2 + 5b^2 \geq 5$ (since $a^2 \geq 0$). So to get 2, we'd need $b = 0$. But there is no integer a such that $a^2 = 2$: $1^2 = 1 < 2$, and $2^2 = 4 > 2$.

   (f) **Explain this implies that the ideal $(2, 1 + \sqrt{-5})$ cannot be principal.**
   If the ideal $(2, 1+\sqrt{-5})$, then its generator would have to have norm dividing the norms of all elements of $(2, 1 + \sqrt{-5})$. Since both 4 and 6 are such norms, the generator would have to have norm 1 or 2. On the other hand, the generator has to have even norm by part (d). And there are no elements of $\mathbb{Z}[\sqrt{-5}]$ of norm 2.

(g) **Show that there are ring isomorphisms**

$$\mathbb{Z}[\sqrt{-5}]/(1+\sqrt{-5}) \cong \mathbb{Z}_6, \quad \textbf{and} \quad \mathbb{Z}[\sqrt{-5}]/(2,1+\sqrt{-5}) \cong \mathbb{Z}_3.$$

Let $\mathbb{Z}_2[\varepsilon]/(\varepsilon^2)$ denote the ring consisting of the four elements $\{0,1,\varepsilon,1+\varepsilon\}$, with $1+1=0$ and $\varepsilon^2=0$ (and of course 0 is the zero element, 1 is the multiplicative unit, etc.). Show that there is a ring isomorphism

$$\mathbb{Z}[\sqrt{-5}]/(2) \cong \mathbb{Z}_2[\varepsilon]/(\varepsilon^2).$$

For the first isomorphism $\mathbb{Z}[\sqrt{-5}]/(1+\sqrt{-5}) \cong \mathbb{Z}_6$, note that $(1-\sqrt{-5})(1+\sqrt{-5}) = 6$, and so the class of $a+b\sqrt{-5} \mod 1+\sqrt{-5}$ depends only on $a, b \mod 6$: you can adjust $a \rightsquigarrow a-6$ by subtracting $(1-\sqrt{-5})(1+\sqrt{-5})$, and you can adjust $b \rightsquigarrow b-6$ by subtracting $\sqrt{-5}(1-\sqrt{-5})(1+\sqrt{-5}) = (5-\sqrt{-5})(1+\sqrt{-5})$. Moreover, the class of $a+b\sqrt{-5} \mod 1+\sqrt{-5}$ manifestly depends only on $a-b$. We claim that the numbers $0,1,2,3,4,5$ are pairwise inequivalent mod $1+\sqrt{-5}$. To show this, it suffices to show that none of their differences are divisible in $\mathbb{Z}[\sqrt{-5}]$ by $1+\sqrt{-5}$. But their differences are $1,2,3,4,5$, with norms $N(1)=1$, $N(2)=4$, $N(3)=9$, $N(4)=16$, and $N(5)=25$, none of which is divisible in $\mathbb{Z}$ by $N(1+\sqrt{-5})=6$.

For the second isomorphism $\mathbb{Z}[\sqrt{-5}]/(2,1+\sqrt{-5}) \cong \mathbb{Z}_3$, we can use the first along with one of the Isomorphism Theorems in the textbook.

For the third isomorphism $\mathbb{Z}[\sqrt{-5}]/(2) \cong \mathbb{Z}_2[\varepsilon]/(\varepsilon^2)$, we first note that the class of $a+b\sqrt{-5} \mod (2)$ depends only on a and $b \mod 2$, so that the elements $0, 1, \sqrt{-5}$, and $1+\sqrt{-5}$ represent a complete list of classes in $\mathbb{Z}[\sqrt{-5}]/(2)$. Either by direct analysis or considering norms, it is easy to see that there are no further relations. Moreover, $(1+\sqrt{-5})^2 = -4+2\sqrt{-5} = 0 \mod (2)$. So sending $1+\sqrt{-5} \mapsto \epsilon$ and $\sqrt{-5} \mapsto 1+\epsilon$ supplies the desired isomorphism.

2. **The *Hurwitz quaternions* are $H := \{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \in \mathbb{H}$ s.t. all $a,b,c,d \in \mathbb{Z}$ or all $a,b,c,d \in \mathbb{Z}+\frac{1}{2}\}$. For example, $\mathbf{i}-2\mathbf{j}$ and $\frac{1}{2}+\frac{3}{2}\mathbf{i}-\frac{7}{2}\mathbf{j}-\frac{5}{2}\mathbf{k}$ are elements of H but $\frac{3}{2}\mathbf{i}$ is not.**

   (a) **Show that H is a (noncommutative!) unital subring of the quaternions $\mathbb{H}$.**
   It is easy to see that H is an additive subgroup of $\mathbb{H}$. The nontrivial statement is that H is closed under multiplication. Let us say that an element $x = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \in H$ is *integral* if $a,b,c,d \in \mathbb{Z}$, and *half-integral* if $a,b,c,d \in \mathbb{Z}+\frac{1}{2}$. We want to show that if $x, y \in H$, then $xy \in H$.
   Since multiplication is distributive, it suffices to select a set that generates H under addition, and then show that $xy \in H$ for any $x, y \in$ our selected set. An example of such a set is the set $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}, \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\}$. Clearly any product of the first four is in H. Also if you multiply any of the first four against $\frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})$, you will get $\frac{1}{2}(\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k})$. The most interesting case is $\left(\frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\right)^2 = \frac{1}{2}(-1+\mathbf{i}+\mathbf{j}+\mathbf{k})$, which is in H.

Recall that the *norm* of a quaternion z is $N(z) = z\bar{z}$, i.e. $N(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}) = a^2+b^2+c^2+d^2$.

   (b) **Show that $N(zw) = N(z)N(w)$ for all $z, w \in \mathbb{H}$.**
   By definition, $N(zw) = (zw)\overline{(zw)}$, where of course $\overline{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}} = a-b\mathbf{i}-c\mathbf{j}-d\mathbf{k}$. Note that $\overline{zw} = \bar{w}\bar{z}$, i.e. $\overline{(-)}$ reverses the order of multiplication. So $N(zw) = zw\bar{w}\bar{z} =$

$zN(w)\bar{z}$. But $N(w) \in \mathbb{R}$, so it commutes with z, and so $N(zw) = zN(w)\bar{z} = z\bar{z}N(w) = N(z)N(w)$.

(c) **Show that $N(z) \in \mathbb{Z}$ for all $z \in H$.**

This is obvious when $z = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ with $a, b, c, d \in \mathbb{Z}$. What about when $a, b, c, d \in \mathbb{Z} + \frac{1}{2}$? Then $N(z)$ is a sum of four squares of elements of $\mathbb{Z} + \frac{1}{2}$. Well, pick $n + \frac{1}{2} \in \mathbb{Z} + \frac{1}{2}$. Then $(n + \frac{1}{2})^2 = n^2 + 2 \cdot n \cdot \frac{1}{2} + (\frac{1}{2})^2 = n^2 + n + \frac{1}{4}$. So we have a sum of four terms each of which is $\frac{1}{4}$ more than an integer, so the sum is an integer.

(d) **Conclude that an element $z \in H$ is invertible if and only if $N(z) = 1$. Describe the group of units $H^\times$. In particular, what are its elements, and how many are there?**

If $z \in H$ has inverse $z^{-1} \in H$, then we must have $1 = N(1) = N(zz^{-1}) = N(z)N(z^{-1})$, which is a product of two (nonnegative!) integers, and so this is only possible if $N(z)$ (and $N(z^{-1})$) is 1.

For the converse, recall that every nonzero element $z \in \mathbb{H}$ is invertible in $\mathbb{H}$ with inverse $z^{-1} = \frac{1}{N(z)}\bar{z}$. If $z \in H$, then $\bar{z} \in H$. Thus for z^{-1} to be in H, it suffices for $N(z) = 1$.

The group $H^\times$ consists of the elements of H of norm 1. Suppose that $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \in H$ with $a, b, c, d \in \mathbb{Z}$. Then the only way for $N(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = a^2 + b^2 + c^2 + d^2$ to be 1 is if one of $a, b, c, d = \pm 1$ and the rest are 0. So that gives a subset of $H^\times$ of order 8, consisting of the elements $\{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$. This is the famous "quaternion group" Q_8.

Now suppose that $a, b, c, d \in \mathbb{Z} + \frac{1}{2}$ and $a^2 + b^2 + c^2 + d^2 = 1$. The smallest value of n^2 for $n \in \mathbb{Z} + \frac{1}{2}$ is $n^2 = \frac{1}{4}$, which occurs only for $n = \pm\frac{1}{2}$. So the smallest value of $a^2 + b^2 + c^2 + d^2$ is $\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$, which occurs only when $a, b, c, d = \pm\frac{1}{2}$. This gives 16 elements in $H^\times$.

All together, we find that $H^\times$ has order $8 + 16 = 24$.

This would suffice to answer the homework exercise, but we can if we want continue on our analysis. By Cauchy's theorem, $H^\times$ contains an element ω of order 3. Let's see if we can find it. It must be of the form $\frac{1}{2}(\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k})$, since the elements of $Q_8 = \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ have order (1 or 2 or) 4. It is not too hard to compute $\frac{1}{2}(\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k})^3$, tracking all the signs carefully, but even easier to compute the square. Why is the square helpful? Because if we are going to have $\omega^3 = 1$, then we will have $\omega^2 = \omega^{-1}$, but every element of $H^\times$ solves $\omega^{-1} = \bar{\omega}$. And upon computing, we find that $\frac{1}{2}(\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k})^2 = \frac{1}{2}(-1 \pm \dots)$ — the real part is always negative. If this is going to be $\bar{\omega}$, then ω itself had better have a negative real part.

So let's try $\omega = \frac{1}{2}(-1+\mathbf{i}+\mathbf{j}+\mathbf{k})$. Then direct computation shows $\omega^2 = \frac{1}{2}(-1-\mathbf{i}-\mathbf{j}-\mathbf{k}) = \bar{\omega}$, and so we have succeeded.

How does this ω relate to the elements of Q_8? Of course, ± 1 are central, and there is a symmetry between $\mathbf{i}, \mathbf{j}, \mathbf{k}$. Direct computation shows $\omega\mathbf{i} = \frac{1}{2}(-\mathbf{i} - 1 + \mathbf{k} - \mathbf{j})$ whereas $\mathbf{i}\omega = \frac{1}{2}(-\mathbf{i} - 1 - \mathbf{k} + \mathbf{j})$. From these and the same for $\mathbf{j}, \mathbf{k}$, we see that

$$\omega\mathbf{i}\omega^{-1} = \mathbf{j}, \quad \omega\mathbf{j}\omega^{-1} = \mathbf{k}, \quad \omega\mathbf{k}\omega^{-1} = \mathbf{i}.$$

This implies that the subgroup $Q_8 \subset H^\times$ is normal, and that the whole group is a semidirect product

$$H^\times = Q_8 \rtimes C_3$$

with the C_3-subgroup generated by ω and acting on Q_8 by the cyclic permutation $\mathbf{i} \mapsto \mathbf{j} \mapsto \mathbf{k} \mapsto \mathbf{i}$.

(e) **Show that the subset $J \subset H$ defined by**

$$J := \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H} \textbf{ s.t. all } a, b, c, d \in \mathbb{Z} \textbf{ and } a + b + c + d \in 2\mathbb{Z}\}$$

is a two-sided ideal.

We consider it obvious that $J \subset H$ is an additive subgroup. We wish to show that J absorbs multiplication from both sides: if $x \in H$ and $y \in J$, then xy and yx are in J. As in part (a), we will do this by letting x range just over a set that generates H as an additive group. An example of such a set is $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}, \omega\}$.

Multiplication of $y = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ on either side by $\mathbf{i}, \mathbf{j}, \mathbf{k}$ has the effect of rearranging the coefficients a, b, c, d and switching some of their signs. This will not change whether they are all in $\mathbb{Z}$, and assuming they are in $\mathbb{Z}$, then it won't change the parity (=remainder mod 2) of their sum (since if $n \in \mathbb{Z}$, and n and $-n$ have the same parity).

The interesting question is to show that $y\omega$ and ωy are in J if y is. We can do this by repeating the trick, now choosing a set that generates J as an additive group. An example of such a set is $\{2, 1 + \mathbf{i}, 1 + \mathbf{j}, 1 + \mathbf{k}\}$. Indeed, integer combinations of the last three can supply any element of the form $(b+c+d) + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ with $b, c, d \in \mathbb{Z}$. Then as long as $a+b+c+d \in 2\mathbb{Z}$, we can add some integer multiple of 2 to get $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$. So we want to show that if $y \in \{2, 1 + \mathbf{i}, 1 + \mathbf{j}, 1 + \mathbf{k}\}$, then $y\omega$ and ωy are in J. Well, $2\omega = \omega 2 = -1 + \mathbf{i} + \mathbf{j} + \mathbf{k}$, which is in J since $-1 + 1 + 1 + 1 = 2 \in 2\mathbb{Z}$. The other products are all essentially the same, so we will report one of them:

$$(1 + \mathbf{i})\omega = -1 + \mathbf{j} \in J.$$

(f) **Calculate the quotient ring H/J. Hint: Show that $|H/J| = 4$. Show that H/J has characteristic 2. Show that H/J contains an element $\omega \neq 1$ such that $\omega^3 = 1$. Conclude that H/J is the finite field $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$.**

We first note that since $2 \in J$, H/J definitely has characteristic 2. Second, we have at various times chosen an additive generating set for H. For any such choice, its image in H/J will again be an additive generating set. For example, H/J is additively generated by the cosets $1 + J, \mathbf{i} + J, \mathbf{j} + J, \mathbf{k} + J, \omega + J$. Note that the first four of these cosets are equal, and not the trivial coset J: they are all the set

$$\{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \text{ s.t. } \text{ s.t. all } a, b, c, d \in \mathbb{Z} \text{ and } a + b + c + d \in 2\mathbb{Z} + 1\}.$$

On the other hand, $\omega + J \neq J$ and $\omega + J \neq 1 + J$.

So H/J consists of the integer combinations of $1 + J$ and $\omega + J$. Since H/J has characteristic 2, the coefficients in these combinations are just 0 and 1. Thus a complete list of cosets is $H/J = \{0 + J, 1 + J, \omega + J, 1 + \omega + J\}$.

One can also see that H/J has order 4 without having earlier found the element ω. Indeed, it is not hard to show that the following is a complete list of cosets:

$$J = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \text{ s.t. } \text{ s.t. all } a, b, c, d \in \mathbb{Z} \text{ and } a + b + c + d \in 2\mathbb{Z}\},$$
$$\{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \text{ s.t. } \text{ s.t. all } a, b, c, d \in \mathbb{Z} \text{ and } a + b + c + d \in 2\mathbb{Z} + 1\},$$
$$\{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \text{ s.t. } \text{ s.t. all } a, b, c, d \in \mathbb{Z} + \tfrac{1}{2} \text{ and } a + b + c + d \in 2\mathbb{Z}\},$$
$$\{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \text{ s.t. } \text{ s.t. all } a, b, c, d \in \mathbb{Z} + \tfrac{1}{2} \text{ and } a + b + c + d \in 2\mathbb{Z} + 1\}.$$

Even without finding ω, we can still invoke Cauchy's theorem to know that H does contain some element $\omega \neq 1 \in H$ such that $\omega^3 = 1$. The image of this element must be

some element of H/J of order three, unless its image is (the class of) 1. Can the latter be the case? Well, $1 + J \cap H^\times$ consists of elements with integer coefficients, and those all have order (1 or 2 or) 4. So no, it cannot be.