MATH 220B: MIDTERM EXAMINATION
FEBRUARY 20, 2018
DANIEL HALMRAST

Problem 1

Let $R = \mathbb{Z}[\sqrt{-d}]$ be the set of all complex numbers of the form $a + b\sqrt{-d}$, where a and b are integers and d is a square-free natural number. Show that R is a ring with four units is $d = 1$ and 2 units otherwise.

Proof. We first show that R is a ring. To do so, we show that R is a subring of the complex numbers $\mathbb{C}$. Namely, we wish to show that R is closed under addition and complex multiplication, and that R contains the unit element 1.

To see that R is closed under addition, we calculate the sum of two arbitrary elements of R, namely $a + b\sqrt{-d}$ and $f + g\sqrt{-d}$ where $a, b, f, g \in \mathbb{Z}$.

$$(a + b\sqrt{-d}) + (f + g\sqrt{-d}) = (a + f) + (b + g)\sqrt{-d}$$

and since $a + f$ and $b + g$ are integers, $(a + f) + (b + g)\sqrt{-d} \in R$ as desired.

Similarly, we calculate the product of two arbitrary elements of R.

$$\begin{aligned}(a + b\sqrt{-d})(f + g\sqrt{-d}) &= af + ag\sqrt{-d} + bf\sqrt{-d} + bg(\sqrt{-d})^2 \\ &= (af - bgd) + (ag + bf)\sqrt{-d}\end{aligned}$$

and since $af - bgd$ and $ag + bf$ are integers, $(af - bgd) + (ag + bf)\sqrt{-d}$ is in R as desired. Thus, R is closed under multiplication.

Finally, since R contains the unit element 1 (as $1 + 0\sqrt{-d}$), R is indeed a subring of $\mathbb{C}$, and is therefore a ring under the same operations.

Now, we wish to show that for $d = 1$, R has four units. Specifically, we will show that the elements $1, -1, \sqrt{-1}, -\sqrt{-1}$ are the only units in $\mathbb{Z}[\sqrt{-1}]$.

First, we observe that $1, -1, \sqrt{-1}$, and $-\sqrt{-1}$ are indeed units. 1 is clearly a unit, since $1 \cdot 1 = 1$, and thus 1 is its own inverse. Similarly, $(-1) \cdot (-1) = 1$, and thus -1 is its own inverse. Finally, we observe that $(\sqrt{-1}) \cdot (-\sqrt{-1}) = 1$ and so $\sqrt{-1}$ and $-\sqrt{-1}$ invert each other. Thus, the four elements $1, -1, \sqrt{-1}, -\sqrt{-1}$ are indeed units in R.

To see these are the only units, we define the function $N : R \to \mathbb{Z}^+$ given by

$$N(z) = z\bar{z}$$

where $\bar{z}$ is the complex conjugate of z. Now, this function is multiplicative in the sense that for $z, w \in R$, $N(zw) = N(z)N(w)$. This is clear, since

$$\begin{aligned} N(zw) &= zw\overline{zw} \\ &= zw\bar{w}\bar{z} \\ &= z\bar{z}w\bar{w} \qquad \text{by commutativity of the multiplication} \\ &= N(z)N(w) \end{aligned}$$

Now, from this definition of N, it is clear that any element $z \neq 0$ of R must have that $N(z) \geq 1$, since

$$N(a + b\sqrt{-1}) = a^2 + b^2$$

which, for integers a and b with at least one nonzero, is always greater than or equal to 1.

Suppose z were a unit in R with inverse w. Then, it would follow that

$$\begin{aligned} zw &= 1 \\ \implies N(zw) &= N(1) = 1 \\ \implies N(z)N(w) &= 1 \end{aligned}$$

and since N can take on only positive integer values, this forces $N(z) = N(w) = 1$. Clearly, the only elements of R which satisfy this property are the elements $1, -1, \sqrt{-1}, -\sqrt{-1}$ since for an element $a + b\sqrt{-1}$ we have

$$N(a + b\sqrt{-1}) = a^2 + b^2$$

and for a number with both a and b nonzero, $N(a + b\sqrt{-1}) \geq 2$.

Thus, the only units in $\mathbb{Z}[\sqrt{-1}]$ are the four elements with $N(z) = 1$, namely $1, -1, \sqrt{-1}, -\sqrt{-1}$.

For $d \neq 1$, we can similarly define the function N as $N(z) = z\bar{z}$. However, in this case there are only two elements that satisfy $N(z) = 1$. To see this, we calculate

$$N(a + b\sqrt{-d}) = a^2 + b^2 d$$

which for $d \geq 2$ is only equal to 1 when $b = 0$ and $a = \pm 1$. Thus, the only two units in $\mathbb{Z}[\sqrt{-d}]$ are 1 and -1 (which are their own inverses, and therefore units as desired). $\square$

Problem 2

Let R be a commutative ring. Give the definition of the nilradical $\mathfrak{N}(R)$. Show that the following are equivalent:

i R has exactly one prime ideal.

ii Every element in R is either a unit or nilpotent.

iii $R/\mathfrak{N}$ is a field.

Proof. The nilradical $\mathfrak{N}$ of R is defined to be the set of all nilpotent elements of R. That is, the set of all elements x for which $x^n = 0$ for some $n \geq 1$.

For this problem, we will also use the following useful lemma:

Lemma. *For a ring R, the nilradical is the intersection of all prime ideals in R.*

Proof. We first show that every nilpotent element is in every prime ideal. So, let $\mathfrak{p}$ be a prime ideal in R, and let x be nilpotent. That is, $x^n = 0$ for some $n \geq 1$. Since $\mathfrak{p}$ contains 0, we know that $x^n \in \mathfrak{p}$.

Now, we prove a general result: for $x \in R$, $m \in \mathbb{N}$, and $x^m \in \mathfrak{p}$ a prime ideal, then $x \in \mathfrak{p}$ as well. This proof will induct on the exponent of x. For the base case, note that if $x^1 \in \mathfrak{p}$, then trivially $x \in \mathfrak{p}$. Now, suppose the result holds for $m = k$, and suppose $x^{k+1} \in \mathfrak{p}$. Then, by primality of $\mathfrak{p}$, it must be that either $x \in \mathfrak{p}$ or $x^k \in \mathfrak{p}$, either of which implies that $x \in \mathfrak{p}$ as desired.

Thus, since $x^n = 0 \in \mathfrak{p}$, it follows that $x \in \mathfrak{p}$ as well. So, every nilpotent element is in every prime ideal of R.

Now, suppose y is not nilpotent, and consider the ideal $\mathfrak{p}$ which is maximal with respect to the property that y^n is not in the ideal for all $n \geq 1$. Such a maximal ideal exists since (0) satisfies the property, and Zorn guarantees a maximal element with respect to that property.

In particular, $\mathfrak{p}$ does not contain y, so all we need to show is that $\mathfrak{p}$ is prime. To do so, let a and b be elements of $R \setminus \mathfrak{p}$. We will show that their product is also not in $\mathfrak{p}$. Now, the ideal $\mathfrak{p} + (a)$ properly contains $\mathfrak{p}$, and so by maximality of p, $\mathfrak{p} + (a)$ must contain some y^n for some $n \geq 1$. Similarly, $\mathfrak{p} + (b)$ contains some y^m for some $m \geq 1$. It follows immediately that y^{n+m} is in $\mathfrak{p} + (ab)$, and since $\mathfrak{p}$ does not contain any power of y, it must be that $\mathfrak{p} + (ab) \neq \mathfrak{p}$ and so $ab \notin \mathfrak{p}$.

Thus, $\mathfrak{p}$ is prime, and so y is not in the intersection of all prime ideals. $\square$

With that in mind, let's prove the equivalences.

(i $\implies$ ii) Suppose R is such that it has exactly one prime ideal. In particular, this means that $\mathfrak{N}$ is the only prime ideal in R. Suppose $x \in R$ is such that x is not a unit. That is, $(x) \neq R$. Now, consider the ideal $\mathfrak{p}$ which is maximal with respect to the property that (x) is contained in the ideal, and 1 is not in the ideal. This exists, since (x) satisfies the property, and Zorn guarantees a maximal element.

Now, $\mathfrak{p}$ is easily seen to be prime, by a similar argument to the one done in the proof of the lemma above. However, this forces $\mathfrak{p}$ to be the nilradical, which implies that x is nilpotent.

Thus, x is either nilpotent or a unit, as desired.

(ii $\implies$ iii) Suppose R is such that every element is either a unit or nilpotent. In particular, this means that $\mathfrak{N}$ is a maximal ideal. This is clear, since any ideal containing an element not in $\mathfrak{N}$ must contain a unit, and thus must be equal to (1).

Since $\mathfrak{N}$ is maximal, $R/\mathfrak{N}$ is a field, as desired. (This follows from the fact that the quotient of a commutative ring by a maximal ideal yields a ring with no ideals other than $(0) = \{0\}$ and (1), which is a field.)

(iii $\implies$ i) Suppose $R/\mathfrak{N}$ is a field. In particular, this means that there are no ideals in $R/\mathfrak{N}$ aside from $(0) = \{0\}$ and (1). By the correspondence theorem for ideals, this means that R has no ideals aside from $\mathfrak{N}$ and (1) which contain $\mathfrak{N}$. Since $\mathfrak{N}$ is the intersection of all prime ideals, it is contained in every prime ideal. It follows that there are no prime ideals properly containing $\mathfrak{N}$, and thus $\mathfrak{N}$ is the only prime ideal in R, as desired. $\square$

Problem 3

Let R be a commutative ring, and let $R[X]$ be the ring of polynomials over R. Let R^R be the set of all functions from R to itself.

Part a. Show how to define a ring structure on R^R in such a way that the map $\phi_R : R[X] \to R^R$ that takes each polynomial $f(X)$ to the function $r \mapsto f(r)$ is a ring homomorphism.

Proof. The ring structure on R^R will be the structure of pointwise addition and multiplication. That is,

$$(f+g)(r) = f(r) + g(r)$$
$$(fg)(r) = f(r)g(r)$$

It is easy to verify that this yields a ring structure, since at each point the addition and multiplication are being done in the base ring. Since the base ring addition and multiplication satisfy the ring axioms, so do the pointwise analogues.

Now, we must check that the map ϕ_R is a ring homomorphism. That is, we wish to show that it respects addition and multiplication, and that it sends the unit element in $R[X]$ to the unit element in R^R.

Let $p(X)$ and $q(X)$ be polynomials in $R[X]$. Then,

$$\begin{aligned}\phi_R(p(X) + q(X)) &= (r \mapsto p(r) + q(r)) \\ &= (r \mapsto p(r)) + (r \mapsto q(r)) \\ &= \phi_R(p(X)) + \phi_R(q(X))\end{aligned}$$

and

$$\begin{aligned}\phi_R(p(X)q(X)) &= (r \mapsto p(r)q(r)) \\ &= (r \mapsto p(r))(r \mapsto q(r)) \\ &= \phi_R(p(X))\phi_R(q(X))\end{aligned}$$

Finally,

$$\phi_R(1) = (r \mapsto 1) = 1$$

and so ϕ_R is a ring homomorphism as desired. □

Part b. Suppose now R is a field, k say. Show that ϕ_k is injective if and only if k is infinite.

Proof. Suppose first that k is finite. Then, the set k^k is also finite. However, the set $k[X]$ is infinite (in particular, it contains $f(X) = X^n$ for each $n \in \mathbb{N}$), and so ϕ_k cannot be injective as a function from an infinite set to a finite set.

Suppose instead that ϕ_k is not injective. Then, there is some polynomial $f(X)$ in the kernel of ϕ_k. In particular, this means that $f(r) = 0$ for all $r \in k$. Now, since f is a polynomial, we can factorize it by its roots as

$$f(X) = C \prod_{r \in k} (X - r)$$

and for f to be of finite degree, there must be only finitely many elements of k to choose from. Thus, ϕ_k not being injective implies that k is finite, as desired. □

Part c. Show that ϕ_k is surjective if and only if k is finite.

Proof. Suppose first that k has n elements, labeled k_i. Then, let $f \in k^k$ be any function, and define $f_i = f(k_i)$. We wish to find a polynomial $p(X)$ for which $p(k_i) = f_i$. This is easily done by setting

$$p(X) = \sum_{i=1}^{n} f_i \frac{\prod_{j \neq i}(X - k_j)}{\prod_{j \neq i}(k_i - k_j)}$$

and so $\phi_k(p(X)) = f$ and ϕ_k is surjective as desired.

Now, suppose k is infinite. Then, the function f defined as

$$f(r) = \begin{cases} 1, & r = 0 \\ 0, & r \neq 0 \end{cases}$$

has infinitely many roots. However, polynomials only have a finite number of roots, and so f is not the image of any polynomial in $k[X]$. Thus, ϕ_k is not surjective as desired. $\square$

Problem 4

Let R be a commutative ring.

Part a. Show that if an R-module is irreducible, then it is cyclic, but not conversely.

Proof. First, note that in the case of the trivial module $\{0\}$, the statement is vacuously true. So, assume the R-module M is not trivial.

Suppose M is an R-module which is irreducible. That is, the only submodules of M are $\{0\}$ and M. Now, let $m \in M$ with $m \neq 0$, and consider the submodule $Rm = \{rm \mid r \in R\}$. This is easily verified to be a submodule. First, we see that it is closed under addition, since for $r, s \in R$, $rm + sm = (r + s)m \in Rm$. Similarly, Rm is closed under multiplication by the ring R, since for $r, s \in R$, $r(sm) = (rs)m \in Rm$. Finally, we note that Rm contains $0m = 0$, and so Rm is a submodule. Since Rm contains $1m = m \neq 0$, it is not the trivial submodule. Since M is irreducible, this implies that $Rm = M$ and so M is cyclic.

To see that the converse is not true, let R be a nonzero ring with a proper ideal $\mathfrak{I}$, and let $M = R$ as an R-module over itself. Then, $M = R1$ and is therefore cyclic, but M contains $\mathfrak{I}$ as a submodule, and is therefore not irreducible. □

Part b. Let M and N be irreducible R-modules. Give a complete description of $\mathrm{Hom}_R(M, N)$.

Proof. Since both M and N are irreducible, they must be cyclic. That is, $M = Rm$ for some $m \in M$ and $N = Rn$ for some $n \in N$. Thus, any map ϕ is determined by where it sends m. To see this, note that

$$\begin{aligned}\phi(x) &= \phi(rm) \quad \text{for some } r \in R \\ &= r\phi(m)\end{aligned}$$

Now, the image of any module homomorphism is a submodule. To see this, let $\psi : M' \to N'$ be an R-module homomorphism. Now, by definition $\psi(1) = 1$ and so $1 \in \text{im}(\psi)$. Furthermore, for $\psi(x), \psi(y)$ in the image,

$$\psi(x) + \psi(y) = \psi(x + y)$$

and so the image is closed under addition. Finally, for any $r \in R$, $r\psi(x) = \psi(rx)$ and so the image is closed under ring multiplication.

By similar reasoning, the kernel of any R-module homomorphism is also a submodule.

Thus, since both M and N are irreducible, the kernel of ϕ in M must be trivial (or the whole thing), and the image of ϕ must be trivial (or the whole thing).

Thus, ϕ is either the zero map, or ϕ is an injective (trivial kernel) surjection onto N (i.e. an isomorphism).

So, for $M = Rm$, ϕ must send m to some element n for which $N = Rn$. In particular, there is a one-to-one correspondence between elements of N for which $N = Rn$ and elements of $\text{Hom}_R(M, N)$ given by $n \mapsto \phi_n$ where ϕ_n is defined by $\phi_n(m) = n$. □