Math 504 HW7

Rohan Mukherjee

December 7, 2023

1. Let $I \subset R$ be an ideal. If $I = (0)$ we are done, so suppose I contains a nonzero element. Define $\mathcal{S} = \{ \sum r_i x_i \mid r_i \in R, x_i \in x \} \setminus 0$. Associate to $\mathcal{S}$ the set $N = \{ N(y) \mid y \in S \}$. N is a nonempty set of $\mathbb{Z}_{\geq 0}$ and hence it has a (not necessarily unique) minimal element d. By definition, there exists an element $z \in \mathcal{S}$ such that $N(z) = d$. We claim of course that $(d) = I$. Suppose otherwise, that there was an element $a \in I$ so that $a \notin (d)$. We have that $a = dq + r$ for some $r = 0$ or $N(r) < N(d)$, but since $a \notin (d)$, we can't have $r = 0$. Notice now that $a - dq$ is an R-linear combination of elements of I, and hence $a - dq \in I$. But then $a - dq = r$ is an element of I with smaller norm than d, a contradiction.

2. (a) We shall show that $\mathbb{Z}[i]$ is a Euclidean Domain. Let $a + bi, c + di \in \mathbb{Z}[i]$ with $c + di \neq 0$. Notice that,

$$\frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + i\frac{bc-ad}{c^2+d^2}$$

Now define $r = \frac{ac+bd}{c^2+d^2} \in \mathbb{Q}$ and $s = \frac{bc-ad}{c^2+d^2} \in \mathbb{Q}$. If both r, s are integers we are done, else the sets $[k, k+1)$ for $k \in \mathbb{Z}$ partition $\mathbb{R}$, so we must have $r \in [k, k+1)$ for some integer k. From here, either $r \in [k, k+1/2)$, or $r \in [k+1/2, k)$. In the first case, we have $|k - r| \leq 1/2$, and in the second we have $|k+1-r| \leq 1/2$, so, possibly replacing k with $k+1$, we have found an integer within $1/2$ of r. Similarly we can find an integer l such that $|l - s| \leq 1/2$. Write $k = r + \varepsilon$ and $l = s + \delta$, where $|\varepsilon| \leq 1/2$ and $|\delta| \leq 1/2$, thus

$$\begin{aligned}
N(a+bi-(k+li)(c+di)) &= N(a+bi-(r+si+\varepsilon+\delta i)(c+di)) \\
&= N(a+bi-a-bi+(\varepsilon+\delta i)(c+di)) = N((\varepsilon+\delta i)(c+di)) \\
&= N(\varepsilon+\delta i)N(c+di) = (\varepsilon^2+\delta^2)N(c+di) \leq \frac{1}{2}N(c+di)
\end{aligned}$$

In particular, $N(a+bi-(k+li)(c+di)) < N(c+di)$, completing the proof.

(b) Let x be a unit. Then $N(xx^{-1}) = N(x)N(x^{-1}) = N(x)N(x^{-1}) = 1$ (We are using elementary facts from complex analysis about $N(a+bi) = a^2+b^2$). The only units in $\mathbb{Z}$ are ± 1, and the only positive one of those is just 1. So, units in $\mathbb{Z}[i]$ are precisely those elements $a+bi \in \mathbb{Z}[i]$ with $N(a+bi) = a^2+b^2 = 1$. From here we can only have $a = \pm 1$ with $b = 0$ or $a = 0$ with $b = \pm 1$. These yield $\pm 1, \pm i$ as the only units.

(c) We first classify which primes are irreducible. $2 = (1+i)(1-i)$, so we reduce to odd primes. If p is an odd prime and is reducible, then $p = ab$ for a, b not units. Then $N(ab) = N(a)N(b) = p^2$, and since we are now working in the integers, we must have $N(a) = p$ (it cannot be 1, else it would be a unit). This would say that $p = x^2+y^2$ for some integers x, y, which is true iff $p \equiv 1 \mod 4$. Now if $p \equiv 3 \mod 4$, then p is not the sum of two squares, so it is irreducible. Now, suppose that x were irreducible, and notice that $x\overline{x} = N(x) = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. Since x is irreducible, we must have $p_1 \in (x)$, thus $p_1 = yx$ for some y. If y is a unit we are done (we are back to the prime case), so suppose otherwise. Then $N(x) = p_1$ through a similar line of reasoning as above. Now we claim that elements with prime order are irreducible. If $x = ab$, with $N(x) = p$, then $N(a)N(b) = N(x) = p$, so one of $N(a), N(b)$ must be 1, i.e. x is irreducible. Thus the irreducible elements in $\mathbb{Z}[i]$ are those with prime order, and primes (in $\mathbb{Z}$) that are congruent to $3 \mod 4$.

3. Define the following norm on $\mathbb{Z}[w]$ as $N(a+bw+cw^2) = \frac{1}{2}((a-b)^2+(b-c)^2+(c-a)^2)$. Notice that,

$$\begin{aligned}(a+bw+cw^2)(a+cw+bw^2) &= a^2+b^2+c^2+w(ab+ac+bc)+w^2(ab+ac+bc)\\ &= a^2+b^2+c^2-ab-bc-ca = \frac{1}{2}\Big((a-b)^2+(b-c)^2+(c-a)^2\Big)\end{aligned}$$

Notice that $\overline{a+bw+cw^2} = a+cw+bw^2$, where $\overline{x+iy}$ is just the normal complex conjugate. Thus the above norm is precisely the same one as for complex numbers, and hence it is multiplicative. Notice also that the norm of a complex number is 0 iff the complex number is 0, and in particular $a+bw+cw^2 = 0$ iff $a = b = c$. We now explicitly calculate the quotient:

$$\begin{aligned}\frac{x+yw+zw^2}{a+bw+cw^2} &= \frac{(x+yw+zw^2)(a+cw+bw^2)}{(a-b)^2+(a-c)^2+(b-c)^2}\\ &= \frac{ax+cx+bz+w(ay+bx+cz)+w^2(az+by+cx)}{(a-b)^2+(a-c)^2+(b-c)^2}\end{aligned}$$

Thus define $p = (ax+cx+bz)/((a-b)^2+(a-c)^2+(b-c)^2), q = (ay+bx+cz)/((a-b)^2+(a-$

$c)^2 + (b-c)^2)$, and $r = (az+by+cx)/((a-b)^2+(a-c)^2+(b-c)^2)$. Find i within 1/2 of p, j within 1/2 of q, and k within 1/2 of r. Write $i = p + \varepsilon_1$, $j = q + \varepsilon_2$, and $k = r + \varepsilon_3$. Now,

$$
\begin{aligned}
&N(x + yw + zw^2 - (i + jw + kw^2 + (\varepsilon_1 + \varepsilon_2 w + \varepsilon_3 w^2))(a + bw + cw^2)) \\
&= N(\varepsilon_1 + \varepsilon_2 w + \varepsilon_3 w^2)N((a + bw + cw^2)) \leq \frac{3}{4}N(a + bw + cw^2)
\end{aligned}
$$

Which completes the proof.

4. Write $f(X) = a_0 + a_1 X + \cdots a_n X^n$ and $g(X) = b_0 + b_1 X + \cdots + b_m X^m$, WLOG $m \leq n$ (otherwise we are already done). Consider $h_1(X) = a_n b_m^{-1} x^{n-m} g(X)$. Then the leading term of $h_1(X)$ is just $a_n b_m^{-1} b_m X^{n-m} X^m = a_n X^m$. Thus, we must have that $f(X) - h_1(X)$ has degree $\leq n-1$. If it has degree less than m we are done, else we can do the same thing as above but with $f(X) - h_1(X)$ taking the place of X to find a function $h_2(X)$ which is a multiple of $g(X)$ canceling the highest order term of $f(X) - h_1(X)$. Thus, $f(X) - h_1(X) - h_2(X)$ has degree at most $\deg(f(X) - h(X)) - 1 \leq n - 2$. We can now repeat this k times until $r(X) = f(X) - \sum_{i=1}^{k} h_i(X)$ has degree less than m or is equivalently 0 (k is finite because in the worst case this process takes $n - m$ steps). Thus, $f(X) = \sum_{i=1}^{k} h_i(X) + r(X)$, and since the h_i are divisible by g, we are done.

5. (a) We prove the claim by induction. The polynomial $a_0 + a_1 X$ has at only one root, because we can solve $a_0 + a_1 x = 0$ where $x \in F$ to get that $x = a_1^{-1} a_0$. Now suppose that a polynomial of degree $n - 1 \geq 0$ has at most $n - 1$ roots, and let $f(X)$ be a polynomial of degree n. If f has no roots we are done, so suppose it had a root, a. Then $f(X) = h(X)(X - a) + r$, where $\deg r < \deg(x - a) = 1$ or $r = 0$. Degree 0 elements are just elements of F, so plugging in $x = a$ will yield $0 = f(a) = h(a)(a - a) + r$, which tells us that $r = 0$. Now, $h(X)$ has at most $n - 1$ roots, thus $f(X) = h(X)(X - a)$ has at most $n - 1 + 1 = n$ roots, which completes the proof.

   (b) Notice first that $f(X)$ has either nonnegative degree or is equivalently 0. In the second case we are done, so suppose the first case. Label its degree $n \geq 0$. If $f(X)$ has degree 0, and is not 0, then it has no roots, so we are done. If $n \geq 1$, then by the last part we proved a polynomial of degree n has at most n roots, but $f(X)$ has infinitely many roots–since $f(x) = 0$ (as a function from $F \to F$) for all $x \in F$. This is a contradiction.

   (c) The counterexample is as follows: $f(X) = X^2 + X \in \mathbb{Z}/2[X]$. Notice that $f(X) = 0$ for all $X \in \mathbb{Z}/2[X]$ but $f \neq 0$ (in $\mathbb{Z}/2[X]$).

6. Let P be a group of order $|p|^2$. Then P is abelian, and in particular, $P \cong \mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$. We claim that $Z(P) \neq \langle 1 \rangle$. By the class equation, if $g_1, \ldots, g_r$ are representatives of the non-central conjugacy classes,

$$|P| = |Z(P)| + \sum_{i=1}^{r} |P : C_{g_i}|$$

Since each $C_{g_i} \neq P$ by hypothesis, we must have $p \mid |C_{g_i}|$, and thus $p \mid |P| - \sum_{i=1}^{r} |P : C_{g_i}| = |Z(P)|$. So, $Z(P) \neq \langle 1 \rangle$, and in particular, $p \mid Z(P)$. We have only two cases for $Z(P)$: p or p^2. In the latter case we are done, so suppose the former. Then $|P/Z(P)| = p$, so $P/Z(P) \cong \mathbb{Z}/p$, and in particular it is cyclic, so P is abelian. Now, either P has an element of order p^2, or all elements have order dividing p. In the first case P is cyclic and isomorphic to $\mathbb{Z}/p^2$. Since the only element with order 1 is e, we can find an element x of order p. Now taking $y \in P - \langle x \rangle$, we can see that $\langle x \rangle < \langle x, y \rangle \leq P$, so in particular $\langle x, y \rangle$ divides p^2 and is not 1 or p, hence it equals p^2 and $\langle x, y \rangle = P$. Since P is abelian, we have $\langle x \rangle \langle y \rangle = \{ x^\alpha y^\beta \mid \alpha, \beta \in \mathbb{Z} \} = \langle x, y \rangle$, and also since P is abelian we have $\langle x \rangle \trianglelefteq P$ and $\langle y \rangle \trianglelefteq P$. Thus $P = \langle x \rangle \times \langle y \rangle = \mathbb{Z}/p \times \mathbb{Z}/p$, and we are done.