

## MATH 551 HOMEWORK 10

### SOLUTIONS

- (1) **Hungerford, III.3.1** Since a PID is a ring with identity, we know that every maximal ideal is prime, so we need only show that every nonzero prime ideal is maximal. Let  $I$  be a nonzero prime ideal in a PID  $R$ . Since  $R$  is a PID,  $I = \langle a \rangle$  for some  $a \in R$ , so  $a$  is prime, and thus irreducible. But  $a$  being irreducible implies that  $I$  is maximal with respect to containment among principal ideals, and thus, since all ideals are principal in  $R$ ,  $I$  is a maximal ideal.
- (2) **Hungerford, III.3.3**
- (a) Let  $u = a + b\sqrt{10}$ ,  $v = c + d\sqrt{10}$ . Then  $uv = (ac + 10bd) - (ad + bc)\sqrt{10}$ , so  $N(uv) = (ac + 10bd)^2 - 10(ad + bc)^2 = a^2c^2 - 10b^2c^2 - 10a^2d^2 + 100b^2d^2 = (a^2 - 10b^2)(c^2 - 10d^2)$ . If  $N(u) = a^2 - 10b^2 = 0$ , then  $a = \pm\sqrt{10}b$ , so since  $a, b \in \mathbb{Z}$  and  $\sqrt{10}$  is irrational,  $a = b = 0$ , so  $u = 0$ .
- (b) If  $u$  is a unit then there is  $v$  with  $uv = 1$ , so  $N(u)N(v) = N(1) = 1$ , so since  $N(u), N(v) \in \mathbb{Z}$  we have  $N(u) = \pm 1$ . Conversely, since  $(a + b\sqrt{10})(a - b\sqrt{10}) = N(a + b\sqrt{10})$ , if  $N(u) = \pm 1$  then  $u$  is a unit.
- (c) We have  $N(2) = 4$ , so if  $2 = uv$  then  $N(u)|4$ , so  $N(u) \in \{\pm 1, \pm 2, \pm 4\}$ . If  $N(u) = \pm 1$ , then  $u$  is a unit, while if  $N(u) = \pm 4$  then  $v$  is a unit, so we just need to show that there is no  $u$  with  $N(u) = \pm 2$ . For such a  $u = a + b\sqrt{10}$ ,  $a^2 - 10b^2 = \pm 2$ , so  $a^2 \equiv \pm 2 \pmod{5}$ . However the only squares modulo 5 are 0 and 1, so no such  $a$  exists. Similarly,  $N(3) = 9$ , so the only possibility for  $3 = uv$  with neither of  $u, v$  units is if  $N(u) = \pm 3$ . But then if  $u = a + b\sqrt{10}$  then  $a^2 - 10b^2 = \pm 3$ , so  $a^2 \equiv \pm 3 \pmod{5}$ , which is impossible as above. Finally,  $N(4 \pm \sqrt{10}) = 6$ , so if  $4 \pm \sqrt{10} = uv$  with neither  $u, v$  units, then  $N(u) \in \{\pm 2, \pm 3\}$ , which is impossible by the above, and similarly for  $4 - \sqrt{10}$ .
- (d) Since  $(2)(3) = (4 + \sqrt{10})(4 - \sqrt{10})$ , if any of 2, 3,  $4 + \sqrt{10}$ ,  $4 - \sqrt{10}$  are prime we would have each of 2, 3 dividing one of

$4 + \sqrt{10}, 4 - \sqrt{10}$  and viceversa. But if  $u$  divides  $v$  then  $N(u)$  divides  $N(v)$ , and 4, 9 do not divide 6 and vice versa.

- (3) **Hungerford, III.3.4** We know by the last part of the previous question that the factorization need not be unique, so we need only show that every nonzero nonunit has a factorization into irreducibles. Since we showed above that 0 is the only element of norm 0, and every element of norm  $\pm 1$  is a unit, it is trivially true that every nonzero nonunit  $u$  with  $|N(u)| < 2$  has a factorization into irreducibles. Now suppose that the same is true for all nonzero nonunits  $u$  with  $|N(u)| < n = |N(v)|$ , with  $n \geq 2$ . We wish to show that the same is true for  $v$ . If  $v$  is irreducible, then it is its own factorization into irreducibles, so we are done. Otherwise we can write  $v = ab$  where neither of  $a$  or  $b$  are units. Then  $N(v) = N(a)N(b)$ , so since neither of  $|N(a)|, |N(b)|$  is one, we must have  $|N(a)|, |N(b)| < n$ , so by the induction hypothesis we can factor both  $a$  and  $b$  into products of irreducibles, so  $v$  is the product of these two decompositions, and can thus be written as a product of irreducibles.

- (4) **Spring 2002** *Call an integral domain  $R$  special if and only if the intersection of any two principal ideals in  $R$  is again principal (generated by one element).*

- (a) *Show that if  $R$  is special, then any two nonzero elements of  $R$  have a greatest common divisor. (An element  $a \in R$  is the greatest common divisor of  $b, c \in R$  if  $a$  divides  $b$ ,  $a$  divides  $c$ , and if  $d \in R$  divides both  $b$  and  $c$ , then  $d$  divides  $a$ .)*

Let  $a, b \in R$ . Then since  $R$  is special there is  $c \in R$  such that  $\langle a \rangle \cap \langle b \rangle = \langle c \rangle$ . Now  $ab \in \langle a \rangle \cap \langle b \rangle$ , so there is  $d \in R$  with  $ab = dc$ . We will show that  $d$  is the greatest common divisor of  $a$  and  $b$ . We also have  $c \in \langle a \rangle$ , so there is  $e \in R$  with  $c = ea$ , and  $c \in \langle b \rangle$ , so there is  $f \in R$  with  $c = fb$ . Thus  $ab = dea$ , so since  $R$  is an integral domain,  $b = de$ , so  $d$  divides  $b$ . Similarly, from  $ab = dfb$  we conclude that  $a = df$ , so  $d$  divides  $a$ . Finally, suppose that  $g$  divides  $a$  and  $g$  divides  $b$ . Then  $a = gr, b = gs$  for  $r, s \in R$ , so  $ab = g^2rs = cd$ , while  $grs \in \langle c \rangle$ , so  $grs = ck$ . Thus  $gck = cd$ , so  $gk = d$ , and thus  $d$  divides  $g$ , so we conclude that  $d$  is a greatest common divisor of  $a$  and  $b$ .

- (b) *Give an example of a special integral domain  $R$  and nonzero elements  $a, b \in R$  such that the greatest common divisor of  $a$  and  $b$  is not an  $R$ -linear combination of  $a$  and  $b$ .*

Let  $R = \mathbb{C}[x, y]$ . The ring  $R$  is an integral domain, and a UFD, so we first show that it is a special integral domain. If  $f = f_1 \dots f_r$  and  $g = g_1 \dots g_s$  are factorizations of  $f, g \in R$  into irreducibles, let  $h = fg / \prod'_k g_k$ , where the product is over those  $g_i$  which are associated to some  $f_i$ . Then  $h \in \langle f \rangle \cap \langle g \rangle$ , and if  $f$  divides  $a$  and  $g$  divides  $b$ , then  $h$  divides  $a$ , so  $\langle f \rangle \cap \langle g \rangle \subseteq \langle h \rangle$ , and thus  $\langle f \rangle \cap \langle g \rangle = \langle h \rangle$ , so  $R$  is special. Note that we only used the fact that  $R$  was a UFD here.

Now let  $x, y \in R$ . Then the greatest common divisor of  $x$  and  $y$  is 1, but  $1 \neq fx + gy$  for any  $f, g \in R$ , since  $1 \notin \langle x, y \rangle$ .

- (5) **Spring 2001** Let  $A$  be the abelian group of quintuples of integers under addition, and let  $G$  be the subgroup generated by the elements

$$(1, -1, 0, 2, 1), (2, 3, 1, 1, 0), (4, 1, 0, 0, 2), (-1, 1, -1, 1, 1), (1, 1, 1, 1, 1).$$

Determine the group  $A/G$  as a product of cyclic groups.

Let  $B$  be the matrix

$$B = \begin{pmatrix} 1 & -1 & 0 & 2 & 1 \\ 2 & 3 & 1 & 1 & 0 \\ 4 & 1 & 0 & 0 & 2 \\ -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Consider the following set of row and column operations: add an integer multiple of one row/column to another row/column, multiply a row/column by  $-1$ , and switch two rows/columns. The row operations correspond to choosing a different set of generators for the group  $G$ , while the column operations correspond to choosing a different basis for  $A$ , so integer row and column operations do not change the quotient  $A/G$ . Now we can reduce the matrix  $B$  using such row and column sums to

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 30 \end{pmatrix}.$$

The exact row and column operations required can be computed from a factorization into elementary operation matrices

of the matrices  $U$  and  $V$  produced by `maple` by the command `ismith(B,U,V)` if  $B$  has been entered as a matrix.

Thus  $A/G$  is isomorphic to  $\mathbb{Z}\langle x_1, x_2, x_3, x_4, x_5 \rangle / \langle x_1, x_2, x_3, 2x_4, 30x_5 \rangle \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$ .

- (6) *Describe an algorithm to answer all questions of the form of the previous question. Hint: You want a computational form of our theorem about subgroups about free abelian groups.*

Given a set of vectors  $H$  in  $\mathbb{Z}^n$ , we want to compute  $\mathbb{Z}^n/G$ , where  $G$  is the subgroup of  $\mathbb{Z}^n$  generated by  $H$ . Form the matrix  $B$  whose rows are the elements of  $H$ . As above, the quotient  $\mathbb{Z}^n/G$  is unchanged by integer row and column operations. By II.I.6 we know that there is a basis  $X = \{x_1, \dots, x_n\}$  for  $\mathbb{Z}^n$  in which  $G$  is generated by  $\{d_i x_i : 1 \leq i \leq n\}$ , where  $d_i \in \mathbb{Z}$  for all  $i$ . Since every element of  $\text{GL}_n(\mathbb{Z})$  can be factored into the matrices corresponding to the integer column operations, we can perform column operations on  $B$  so that the columns of  $B$  correspond to the basis  $X$ .

We now show that we can do integer row operations on  $B$  so that the  $i$ th row is  $d_i x_i$ . Beginning with  $d_1 x_1$ , we note that since  $d_1 x_1 \in G$ , it lies in the integer row space of  $B$ , so we can perform row operations to get the first row to be  $d_1 x_1$  (if  $d_1 x_1 = \sum \lambda_i r_i$ , where  $r_i$  is the  $i$ th row, then add  $(\lambda_1 - 1)/\lambda_2$  times row one to row two, and then add  $\lambda_i$  times row  $i$  to row one for  $2 \leq i \leq n$ ). We know that if  $\sum_{i=1}^k a_i x_i \in G$ , then  $d_1$  divides  $a_1$ , so we can perform integer row operations to get a zero in the first entry of every other row. Now consider  $d_2 x_2$ . This again lies in the row space of the transformed  $B$ , but since the only nonzero entry in the first column is  $d_1$ , and the first column of  $d_2 x_2$  is zero, the expression of  $d_2 x_2$  in terms of the rows of  $B$  cannot use the first row. Thus we can write  $d_2 x_2$  in terms of the sub matrix with the first row and column removed. This proceeds as above. In this fashion we can get  $d_i x_i$  as the  $i$ th row of  $B$ . If more rows of  $B$  remain, we can ensure that they are zero using integer row operations as above (since the  $d_i x_i$  generate  $G$ ).

The previous paragraph showed that it is possible to do integer row and column operations on the matrix  $B$  to bring it to a diagonal form. This forms the basis for the algorithm found in the appendix on page 343 of Hungerford.

- (7) **Berkeley Prelim Spring 1999** *Let  $G$  be a finite group with identity  $e$ . Suppose that for all  $a, b \in G$  distinct from  $e$  there is*

an automorphism  $\sigma$  of  $G$  such that  $\sigma(a) = b$ . Prove that  $G$  is abelian. (Added): Give an example of such a group.

We first note that if  $\phi : G \rightarrow G$  is an automorphism, then  $a$  and  $\phi(a)$  have the same order (since if  $a^n = e$ , then  $\phi(a)^n = \phi(a^n) = e$ , and if  $\phi(a)^n = e = \phi(a^n)$ , then since  $\phi$  is an injection  $a^n = e$ ). So all nonzero elements of  $G$  have the same order. Now by Cauchy's theorem if  $p$  divides  $|G|$  then there is an element  $a \in G$  of order  $p$ , so we conclude that there cannot be two distinct primes dividing  $|G|$ , so  $|G| = p^k$  for some  $k$ . Now we know the center of a nontrivial  $p$ -group is nontrivial, so there is  $g \neq e$  with  $g \in C(G)$ . Then for  $a, b \in R$ , pick an automorphism  $\phi$  with  $\phi(g) = a$ . Then  $ab = \phi(g)b = \phi(g\phi^{-1}(b)) = \phi(\phi^{-1}(b)g) = b\phi(g) = ba$ , so  $G$  is abelian.

An example of such a group is  $\mathbb{Z}/p\mathbb{Z}$  (or indeed  $\bigoplus_{i=1}^k \mathbb{Z}/p\mathbb{Z}$ ) for  $p$  prime.