Homework 3 Solutions

Enrique Treviño

Most problems below are from Judson.

1. The Gaussian integers, $\mathbb{Z}[i]$, are a UFD. Factor each of the following elements in $\mathbb{Z}[i]$ into a product of irreducibles.

   (a) 5
   (b) $1+3i$
   (c) $6+8i$
   (d) 2

   Solution 1.

   (a) $5=(2+i)(2-i)$
   (b) $1+3i=(1+i)(2+i)$
   (c) $6+8i=2(3+4i)=(1+i)(1-i)(3+4i)=(1+i)(1-i)(2+i)^2$.
   (d) $2=(1+i)(1-i)$

2. Let D be an integral domain.

   (a) Prove that F_D is an abelian group under the operation of addition.
   (b) Show that the operation of multiplication is well-defined in the field of fractions, F_D.
   (c) Verify the associative and commutative properties for multiplication in F_D.

   Solution 2. Recall that the operations are $(a,b)+(c,d)=(ad+bc,bd)$, and $(a,b)\cdot(c,d)=(ac,bd)$.

   (a) Commutativity is inherited from D, since $ad=da, bc=cb, bd=db, ad+bc=bc+ad$, so

   $$(ad+bc,bd)=(cb+da,db)=(c,d)+(a,b).$$

   Associativity is because the following two are equal:

   $$((a,b)+(c,d))+(e,f)=(ad+bc,bd)+(e,f)=(adf+bcf+bde,bdf),$$

   $$(a,b)+((c,d)+(e,f))=(a,b)+(cf+de,df)=(adf+bcf+bde,bdf).$$

   The identity is $(0,1)$. Indeed $(a,b)+(0,1)=(a\cdot 1+b\cdot 0,b\cdot 1)=(a,b)$. The inverse of (a,b) is $(-a,b)$, indeed $(a,b)+(-a,b)=(ab+(-ab),b^2)=(0,b^2)=(0,1)$. The last equality is because $(a,b)=(c,d)$ if $ad=bc$ and we have $0\cdot 1=b^2\cdot 0$. Therefore, it's an abelian group.

   (b) Suppose $(a,b)\sim(a',b'),(c,d)\sim(c',d')$, i.e. $ab'=a'b, cd'=c'd$. We want to show $(a,b)\cdot(c,d)\sim(a',b')\cdot(c',d')$. We want to show $(ac,bd)\sim(a'c',b'd')$, but for that we only need to verify $acb'd'=a'c'bd$ and this is true because $ab'=a'b$ and $cd'=c'd$.

   (c) We have

   $$((a,b)\cdot(c,d))\cdot(e,f)=(ac,bd)\cdot(e,f)=(ace,bdf),$$

   and

   $$(a,b)\cdot((c,d)\cdot(e,f))=(a,b)\cdot(ce,df)=(ace,bdf).$$

   Therefore, the operation is associative.

   $$(a,b)\cdot(c,d)=(ac,bd)=(ca,db=(c,d)\cdot(a,b).$$

   Therefore, it is commutative.

3. Prove or disprove: Any subring of a field F containing 1 is an integral domain.

Solution 3. Let D be a subring of F with identity. To be an integral domain we need to show D is commutative and that it has no zero divisors. Since F is a field, it is commutative, therefore D is commutative. Suppose $ab = 0$ with $a, b \in D$. Since $D \subseteq F$, then $a, b \in F$. Suppose $a \neq 0$. Then there is $a^{-1} \in F$. Therefore $a^{-1}(ab) = b$. But the product is also 0. Therefore $b = 0$.

Alternatively, one could see that if $ab = 0$ with $a, b \neq 0$, then there would be such a solution in F. But F is an integral domain. Contradiction!

4. Prove or disprove: If D is an integral domain, then every prime element in D is also irreducible in D.

Solution 4. Suppose $p \in D$ is prime. Suppose p is not irreducible, so $p = ab$ for some nonunits a, b. We know $p|ab$, so $p|a$ or $p|b$. If $p|a$, then $a = pk$. Therefore $p = ab = (pk)b = p(kb)$. Therefore $kb = 1$. Therefore b is a unit. Therefore p is irreducible.

5. Let p be prime and denote the field of fractions of $\mathbb{Z}_p[x]$ by $\mathbb{Z}_p(x)$. Prove that $\mathbb{Z}_p(x)$ is an infinite field of characteristic p.

Solution 5. Let $q(x) \in \mathbb{Z}_p[x]$. Then $q(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ for some $a_i \in \mathbb{Z}_p$. Then $p \cdot q(x) = (a_n p)x^n + (a_{n-1}p)x^{n-1} + \cdots + (a_1 p)x + (a_0 p) \equiv 0$ since $a_i p \equiv 0 \mod p$. Therefore, $\mathbb{Z}_p[x]$ has characteristic p.

That $\mathbb{Z}_p[x]$ is infinite comes from the fact that it contains $1, 1 + x, 1 + x + x^2, \cdots$, which are infinitely many elements.

6. Let $\mathbb{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

   (a) Prove that $\mathbb{Z}[\sqrt{2}\,]$ is an integral domain.

   (b) Find all of the units in $\mathbb{Z}[\sqrt{2}\,]$.

   (c) Determine the field of fractions of $\mathbb{Z}[\sqrt{2}\,]$.

   (d) Prove that $\mathbb{Z}[\sqrt{2}i]$ is a Euclidean domain under the Euclidean valuation $\nu(a + b\sqrt{2}\,i) = a^2 + 2b^2$.

Solution 6.

(a) Since $\mathbb{Q}(\sqrt{2})$ is a field, then $\mathbb{Z}[\sqrt{2}]$ is an integral domain. Indeed, if $a + bi$ was a zero divisor in $\mathbb{Z}[\sqrt{2}]$, then it would also be a zero divisor in $\mathbb{Q}[\sqrt{2}]$.

(b) Let $N(a + b\sqrt{2}) = |a^2 - 2b^2|$. Note

$$\begin{aligned} N((a + b\sqrt{2})(c + d\sqrt{2})) &= N((ac + 2bd) + (ad + bc)\sqrt{2}) \\ &= |(ac + 2bd)^2 - 2(ad + bc)^2| = |a^2c^2 + 4abcd + 4b^2d^2 - 2a^2d^2 - 4abcd - 2b^2c^2|, \end{aligned}$$

and

$$N(a + b\sqrt{2})N(c + d\sqrt{2}) = |a^2 - 2b^2||c^2 - 2d^2| = |a^2c^2 + 4b^2d^2 - 2b^2c^2 - 2a^2d^2|$$

Therefore $N((a + bi)(c + di)) = N(a + bi)N(c + di)$.

In particular, if u is a unit, we have $N(a + bi) = N((a + bi)u) = N(a + bi)N(u)$. Therefore $N(u) = 1$ (unless $N(a + bi) = 0$, which means $a = b = 0$ because if at least one of a, b it not zero and $a^2 - 2b^2 = 0$, then $\sqrt{2} \in \mathbb{Q}$, which is impossible).

Therefore, we are looking for solutions to the equation $|a^2 - 2b^2| = 1$. The equation $a^2 - 2b^2 = 1$ is a Pell equation. One solution is $a = 3, b = 2$. From this, we can consider $(3 + 2\sqrt{2})^n$. Since $N(3 + 2\sqrt{2}) = 1$, then $N((3 + 2\sqrt{2})^n) = 1$. All of these are units (and one can show that they are the only units satisfying $a^2 - 2b^2 = 1$. To have $a^2 - 2b^2 = -1$, we can choose $a = b = 1$. Then $(1 + \sqrt{2})(3 + 2\sqrt{2})^n$ are all units. In fact $(3 + 2\sqrt{2}) = (1 + \sqrt{2})^2$. Therefore, the units are all the powers of $(1 + \sqrt{2})$. But we must also consider their conjugates, their negatives and the negatives of their conjugates. For example, $3 + 2\sqrt{2}, 3 - 2\sqrt{2}, -3 + 2\sqrt{2}, -3 - 2\sqrt{2}$. These are all the units.

(c) The elements have the form $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$, i.e.

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{c^2-2d^2} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

Let $p/q + (r/s)i \in \mathbb{Q}[\sqrt{2}]$, i.e., $a, b, c, d \in \mathbb{Z}$ with $c, d \neq 0$. We want to find a, b, c, d such that

$$\frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2} = \frac{p}{q} + \frac{r}{s}\sqrt{2} = \frac{ps+qr\sqrt{2}}{qs} = \frac{pqs^2+q^2rs\sqrt{2}}{q^2s^2}.$$

Let $d = 0$. Let $c = qs$. We want $ac = pqs^2$ and $bc = q^2rs$, so $a = ps$ and $b = qr$. Grabbing $a = ps, b = qr, c = qs, d = 0$ we have

$$\frac{a+bi}{c+di} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2} = \frac{ac}{c^2} + \frac{bc}{c^2}\sqrt{2} = \frac{a}{c} + \frac{b}{c}\sqrt{2} = \frac{p}{q} + \frac{r}{s}\sqrt{2}.$$

Therefore $\mathbb{Q}[\sqrt{2}] = \mathbb{F}_{\mathbb{Z}[\sqrt{2}]}$.

(d) Let $a + b\sqrt{2}i, c + d\sqrt{2}i \in \mathbb{Z}[\sqrt{2}i]$, with c, d not both zero.

$$\frac{a+b\sqrt{2}i}{c+d\sqrt{2}i} = \frac{(a+b\sqrt{2}i)(c-d\sqrt{2}i)}{c^2+2d^2} = \frac{ac+2bd}{c^2+2d^2} + \frac{bc-ad}{c^2+2d^2}\sqrt{2}i.$$

Let m, n be the closest integers to $\frac{ac+2bd}{c^2+2d^2}$, and $\frac{bc-ad}{c^2+2d^2}$, respectively. Then there exist rationals $r, s \leq 1/2$ such that

$$\frac{a+b\sqrt{2}i}{c+d\sqrt{2}i} = (m+n\sqrt{2}i) + (r+s\sqrt{2}i).$$

Then

$$\begin{aligned} a+b\sqrt{2}i &= (m+n\sqrt{2}i)(c+d\sqrt{2}i) + (r+s\sqrt{2}i)(c+d\sqrt{2}i) \\ &= (m+n\sqrt{2}i)(c+d\sqrt{2}i) + ((rc+2ds) + (sc+rd)\sqrt{2}i). \end{aligned}$$

Since $a+b\sqrt{2}i \in \mathbb{Z}[\sqrt{2}i]$ and $(m+n\sqrt{2}i)(c+d\sqrt{2}i) \in \mathbb{Z}[\sqrt{2}i]$, then $(r+s\sqrt{2}i)(c+d\sqrt{2}i) \in \mathbb{Z}[\sqrt{2}i]$. But then we have our division algorithm. Note that

$$\begin{aligned} \nu((r+s\sqrt{2}i)(c+d\sqrt{2}i)) = (r^2+2s^2)(c^2+2d^2) &\leq \left(\left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2\right)\nu(c+d\sqrt{2}i) \\ &= \frac{3}{4}\nu(c+d\sqrt{2}i) < \nu(c+d\sqrt{2}i). \end{aligned}$$

7. Let D be a Euclidean domain with Euclidean valuation ν. If u is a unit in D, show that $\nu(u) = \nu(1)$.

Solution 7. The rules are that $\nu(a) \leq \nu(ab)$ for any nonzero b and that for any $a, b \neq 0$, there exist q, r such that $a = bq + r$ with $r = 0$ or $\nu(r) < \nu(b)$. Let u be a unit. Then $u \neq 0$. Then $1 = uu^{-1}$. But $\nu(u) \leq \nu(uu^{-1})$, so $\nu(u) \leq \nu(1)$. Similarly $\nu(1) \leq \nu(1 \cdot u) = \nu(u)$. Therefore $\nu(1) \leq \nu(u)$. Therefore $\nu(1) = \nu(u)$.

8. An ideal of a commutative ring R is said to be **finitely generated** if there exist elements $a_1, \dots, a_n$ in R such that every element $r \in R$ can be written as $a_1r_1 + \cdots + a_nr_n$ for some $r_1, \dots, r_n$ in R. Prove that R satisfies the ascending chain condition if and only if every ideal of R is finitely generated.

Solution 8. Let's first prove that if R satisfies the ascending chain condition, then every ideal of R is finitely generated. Let I be a nonzero ideal (the zero ideal is finitely generated since it's $\{0\} = \langle 0 \rangle$). Let a_1 be a nonzero element of I. If $I = \langle a_1 \rangle$, then I is finitely generated. If not, then $I_1 = \langle a_1 \rangle$ is a subset of I. Now consider $a_2 \in I \setminus I_1$ (an element of I that is not in I_1). Let $I_2 = \langle a_1, a_2 \rangle$. If $I = I_2$, then I is finitely generated. Otherwise, there exists $a_3 \in I \setminus I_2$. Let $I_3 = \langle a_1, a_2, a_3 \rangle$. We can continue this process. So we have

$$I_1 \subseteq I_2 \subseteq I_3 \cdots .$$

By the ascending chain condition, there is an N such that for all $n \geq N$, $I_n = I_N$. But if $I_{N+1} = I_N$ that means that there are no elements of I not in I_N, therefore $I = \langle a_1, a_2, \ldots, a_N \rangle$, so I is finitely generated.

For the converse, suppose every ideal of R is finitely generated. Now consider an ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots .$$

As proved in class $I = \bigcup_{i=1}^{\infty} I_i$ is an ideal. But since every ideal is finitely generated, then $I = \langle a_1, a_2, \ldots, a_k \rangle$. But then, for $i = 1, 2, 3, \ldots, k$, $a_i \in I_{j_i}$ for some positive integer j_i. Let $N = \max\{j_1, j_2, \ldots, j_k\}$. Then $a_i \in I_{j_i} \subseteq I_N$ because $j_i \leq N$. Therefore

$$I = \langle a_1, a_2, \ldots, a_k \rangle \subseteq I_N.$$

Therefore $I_n = I_N$ for all $n \geq N$.

9. Let R be a PID. Let P be a prime ideal of R. Prove that R/P is a PID.

   Solution 9. Let I be a nonzero ideal of R/P (the zero ideal is principal). The elements of I are of the form $r + P$ for some $r \in P$. Let $J = \{r \,|\, r + P \in I\}$. Let's show J is an ideal of R. Let $j \in J$ and $s \in J$, then $j + P \in I$ and $s + P \in I$, so $(j + P) - (s + P) \in I$. But $(j + P) - (s + P) = (j - s) + P$. Therefore $j - s \in J$. If $r \in R$, then $rj + P = (r + P)(j + P) \in I$. Therefore $rj \in J$. Therefore J is an ideal of R. Since R is a PID, then $J = \langle j \rangle$ for some $j \in J$. But then for any $i + P \in I$, $i \in \langle j \rangle$, so $i = jk$ for $k \in R$, so $(i + P) = (k + P)(j + P)$, so $(i + P) \in \langle j + P \rangle$. Therefore $I = \langle < j + P \rangle$.

   The only thing left to do to prove that R/P is a PID is to confirm that it is an integral domain. Suppose that $(i + P)(j + P) = 0$. Then $ij + P = 0$, so $ij \in P$. Since P is a prime ideal, then $i \in P$ or $j \in P$. In the first case $i + P = 0$, in the second $j + P = 0$. Therefore R/P is an integral domain.

10. (a) Prove that $\mathbb{Z}[i]/\langle 1 + i \rangle$ is a field of order 2.

    (b) Let $q \in \mathbb{Z}$ be a prime with $q \equiv 3 \bmod 4$. Prove that $\mathbb{Z}[i]/\langle q \rangle$ is a field with q^2 elements.

    Solution 10.

    (a) Let's illustrate by doing the division algorithm on $7 + 12i$ with $1 + i$.

    $$\frac{7 + 12i}{1 + i} = \frac{(7 + 12i)(1 - i)}{2} = \frac{19 + 5i}{2} = \frac{19}{2} + \frac{5}{2}i = (9 + 2i) + \left(\frac{1}{2} + \frac{1}{2}i\right).$$

    Therefore

    $$7 + 12i = (1 + i)(9 + 2i) + (1 + i)\left(\frac{1}{2} + \frac{1}{2}i\right) = (1 + i)(9 + 2i) + i.$$

    Therefore $7 + 12i \equiv i \bmod \langle 1 + i \rangle$.
    In general,

    $$\frac{a + bi}{1 + i} = \frac{(a + bi)(1 - i)}{2} = \frac{a + b}{2} + \frac{b - a}{2}i.$$

    If a, b are both of the same parity, then $\frac{a+b}{2}$ and $\frac{b-a}{2}$ are integers, so $a + bi \in \langle 1 + i \rangle$. If a and b have different parity, then

    $$a + bi = \left(\frac{a + b - 1}{2} + \frac{b - a - 1}{2}\right)(1 + i) + (1 + i)\left(\frac{1}{2} + \frac{1}{2}i\right) = (c + di)(1 + i) + i,$$

    for $c, d \in \mathbb{Z}$. Therefore $a + bi \equiv i \bmod \langle 1 + i \rangle$. This means that $\mathbb{Z}[i]/\langle 1 + i \rangle$ has two elements $\{0, i\}$. A ring with two elements is a field of order 2.

(b) Since $q \equiv 3 \bmod 4$ and q is prime, then q is irreducible in $\mathbb{Z}[i]$, so $\langle q \rangle$ is a maximal ideal (indeed, if $\langle q \rangle \subseteq I \subseteq \mathbb{Z}[i]$, then because $\mathbb{Z}[i]$ is a PID, $I = \langle i \rangle$, but then $i|q$, so i is a unit or i is associate to q, i.e. $I = \mathbb{Z}[i]$ or $I = \langle q \rangle$). Therefore $\mathbb{Z}[i]/\langle q \rangle$ is a field. Now, the reasons it has q^2 elements is that for any $a, b \in \mathbb{Z}_q$, $a + bi$ is different modulo $\langle q \rangle$ because if $a \not\equiv c \bmod q$ and $b \not\equiv d \bmod q$, then $(a-c) + (b-d)i \not\equiv 0 \bmod q$. Therefore, we have at least q^2 distinct elements in $\mathbb{Z}[i]/\langle q \rangle$. The reasons we don't have more is that with $q^2 + 1$ elements of $\mathbb{Z}[i]$, by Pigeonhole principle, two of them must satisfy $a \equiv c \bmod q$ and $b \equiv d \bmod q$, but then $a + bi \equiv c + di \bmod q$. Therefore, there can't be more than q^2 elements, so the field has precidely q^2 elements.