Math 30810 Honors Algebra 3
Homework 13

Andrei Jorza

Due at noon on Thursday, December 8

Do 7 of the following questions. Some questions are obligatory. Artin a.b.c means chapter a, section b, exercise c. You may use any problem to solve any other problem.

1. (You have to do this problem) Let R be a ring and I an ideal of R. Define $J = \{x \in R \mid x^n \in I \text{ for some } n\}$.

   (a) Show that J is an ideal of R as well.

   (b) What is J when $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ for a positive integer n?

   Proof. (a): Suppose $x^m \in I$ and $y^n \in I$. Have $(x+y)^{m+n} = \sum \binom{m+n}{k} x^k y^{m+n-k}$. Since either $k \geq m$ of $m+n-k \geq n$ it follows that $x^k y^{m+n-k} \in I$ so J is closed under addition. If $x^m \in I$ and $r \in R$ then $(rx)^m = r^m x^m \in I$ so J is an ideal.

   (b): $J = \{k \in \mathbb{Z} \mid n \mid k^e \text{ for some } e\}$. Looking at prime factorizations this is equivalent to n and k have the same prime factors. Therefore if $n = p_1^{k_1} \cdots p_r^{k_r}$ is the prime factorization of n then $J = p_1 p_2 \cdots p_r \mathbb{Z}$. ☐

2. Let R be a ring and $N = \{x \in R \mid x^n = 0 \text{ for some } n\}$. The previous problem applied to the 0 ideal shows that N is an ideal of R. Show that N is contained in every prime ideal of R. [Hint: Use the definitions.] (In fact one can show that N equals the intersection of all the prime ideals of R.)

   Proof. Let $\mathfrak{p}$ be any prime ideal of R and $x \in N$. Since $x^n = 0$ in R it follows that $x^n = 0$ in the domain $R/\mathfrak{p}$ as well. But then $x = 0$ in $R/\mathfrak{p}$ as $R/\mathfrak{p}$ is a domain. We deduce that $x \in \mathfrak{p}$. ☐

3. (You have to do this problem) Let R be a ring.

   (a) Show that if x is contained in every maximal ideal of R then $1 + xR \subset R^\times$. [Hint: Every proper ideal is contained in some maximal ideal.]

   (b) Show that if $x \in R$ has the property that $1 + xR \subset R^\times$ then x is contained in every maximal ideal of R. [Hint: if $\mathfrak{m}$ is a maximal ideal which doesn't contain x look at $\mathfrak{m} + (x)$.]

   Proof. (a): Let $y \in R$. We need to show that $1 + xy \in R^\times$. If not then from class we know that $1 + xy$ is in some maximal ideal $\mathfrak{m}$ of R. But $x \in \mathfrak{m}$ by choice so $1 = 1 + xy - x \cdot y \in \mathfrak{m}$ as well which contradicts the fact that maximal ideals are not the unit ideal.

   (b): Follow the hint and suppose $x \notin \mathfrak{m}$ for a maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} \subsetneq \mathfrak{m} + (x) \subset R$ and maximality of $\mathfrak{m}$ and the lemma from class implies that $\mathfrak{m} + (x) = R$. But then $x + y = 1$ for some $y \in \mathfrak{m}$. But then $y = 1 - x = 1 + x \cdot (-1) \notin R^\times$ as otherwise $\mathfrak{m}$ would be the unit ideal. ☐

4. Suppose R is a ring and $\mathcal{S}$ is an ascending chain of ideals of R, i.e., there exists a totally ordered index set $\mathcal{I}$ such that $\mathcal{S} = \{I_i\}_{i \in \mathcal{I}}$ with $I_i \subset I_j$ whenever $i < j$ in $\mathcal{I}$. Show that $\bigcup_{i \in \mathcal{I}} I_i$ is an ideal of R.

Proof. Suppose $x, y \in J = \bigcup I_i$. Then $x \in I_i$ and $y \in I_j$ for some indices i, j. We may assume $i \leq j$ as $\mathcal{I}$ is totally ordered and so $x \in I_j$ as well. Then $x + y \in I_j \subset J$ so J is closed under addition. If $x \in J$ and $r \in R$ then $x \in I_i$ for some i and so $rx \in I_i \subset J$ as well. We deduce that J is an ideal. $\square$

5. Show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain. [Hint: Use the complex distance function.]

Proof. Write $\alpha = \sqrt{-2}$. Define $d(a + b\alpha) = |a + b\alpha|^2 = a^2 + 2b^2$. Then $d(z) = 0$ iff $z = 0$ as $z \in \mathbb{C}$ and $d(R - 0) \subset \mathbb{Z}_{\geq 1}$ by construction.

It remains to show that R satisfies division with remainder with respect to d. Look at the complex number a/b and let $q \in \mathbb{Z}[\alpha]$ be the point of the lattice $\mathbb{Z}[\sqrt{-2}]$ which is closest in Euclidean distance to the complex number a/b. Then a/b lies in a $1 \times \sqrt{2}$ rectangle and thus the closest vertex is at a distance at most $\sqrt{3}/2 < 1$. We conclude that $|a/b - q| < 1$ and defining $r = a - bq$ we deduce that $|r/b| = |a/b - q| < 1$ and so $d(r) = |r|^2 < |b|^2 = d(b)$ as desired. $\square$

6-7 (Counts as 2 problems) Let $R = \mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ with fraction field $F = \mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$.

(a) Show that $d(x + y\sqrt{2}) = |x^2 - 2y^2|$ is multiplicative on $\mathbb{Q}(\sqrt{2})$ and $d(z) = 0$ iff $z = 0$.

(b) Suppose $a, b \in \mathbb{Z}[\sqrt{2}]$ and write $z = a/b = u + v\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Let m be the integer closest to u and n be the integer closest to v. Show that if $q = m + n\sqrt{2}$ then $a = bq + r$ for $d(r) < d(b)$ and conclude that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

Proof. (a): $d((x + y\sqrt{2})(z + t\sqrt{2})) = d(xy + 2zt + (xt + yz)\sqrt{2}) = |(xy + 2zt)^2 - 2(xt + yz)^2|$ while $d(x + y\sqrt{2})(d(z + t\sqrt{2}) = |(x^2 - 2y^2)(z^2 - 2t^2)|$. Breaking up parantheses immediately yields equality.

(b): Let m and n as in the problem. We need to show that $d(r) < d(b)$ which, by part (a), is equivalent to $d(r/b) = d(a/b - q) < 1$. But

$$d(a/b - q) = d(u - m + (v - m)\sqrt{2} = |(u - m)^2 - 2(v - n)^2| \leq (u - m)^2 + 2(v - n)^2 \leq \frac{1}{4} + 2\frac{1}{4} < 1$$

$\square$

8-10 (Counts as 3 problems) Consider the ring $R = \mathbb{Z}[\zeta]$ where $\zeta = e^{2\pi i/3}$.

(a) Show that if $m^2 + mn + n^2 = 1$ then $m - n\zeta \in \mathbb{Z}[\zeta]^\times$ and if $m^2 + mn + n^2$ is a prime integer then $m - n\zeta$ and $m - n\zeta^2$ are irreducible in $\mathbb{Z}[\zeta]$. [Hint: Use $|\cdot|^2$.]

(b) Show that $3 = (1 - \zeta)(1 - \zeta^2)$ and $1 - \zeta$ and $1 - \zeta^2$ are irreducible elements of $\mathbb{Z}[\zeta]$.

(c) Let $p \neq 3$ be a prime integer. Show that if $p \equiv 2 \pmod 3$ then p is irreducible in $\mathbb{Z}[\zeta]$.

(d) Show that if $p \equiv 1 \pmod 3$ is a prime integer then $p \mid x^2 + x + 1$ for some integer x.

(e) Deduce that if $p \equiv 1 \pmod 3$ is a prime integer then $p = m^2 + mn + n^2$ for some integers m and n and therefore that $p = (m - n\zeta)(m - n\zeta^2)$ with $m - n\zeta$ and $m - n\zeta^2$ irreducibles in $\mathbb{Z}[\zeta]$.

Proof. (a): Note that $|m - n\zeta|^2 = (m - n\zeta)(m - n\zeta^2) = m^2 + mn + n^2$. Thus $m^2 + mn + n^2 = 1$ iff $|m - n\zeta| = 1$. As in class if $z \in \mathbb{Z}[\zeta]$ and $|z| = 1$ then $z\overline{z} = 1$ so z is invertible. The opposite direction also holds: if $zy = 1$ then $|z|^2|y|^2 = 1$ and $|z|^2$ is a positive integer divisor of 1 so it has to be 1. If $z = m - n\zeta$ has $|z|^2 = m^2 + mn + n^2 = p$ is a prime and $z = xy$ then $|x|^2|y|^2 = |z|^2 = p$ then one of $|x|^2$ and $|y|^2$ is 1 and so x or y is a unit. We deduce that z is irreducible.

(b): We have $|1 - \zeta|^2 = |1 - \zeta^2|^2 = 3$ and the first half of (b) is immediate and part (a) implies the second half of (b). As a remark $1 - \zeta^2 = -\zeta^2(1 - \zeta)$ so $1 - \zeta$ and $1 - \zeta^2$ form the same prime ideal and $3 = -\zeta^2(1 - \zeta)^2$.

(c): If $p = xy$ is a product of non-units in $\mathbb{Z}[\zeta]$ then $|p|^2 = p^2 = |x|^2|y|^2$ with $|x|^2, |y|^2 \neq 1$. We deduce that $|x|^2 = |y|^2 = p$. But if $x = m - n\zeta$ we'd get $m^2 + mn + n^2 = p$ and so $\equiv 0 \pmod p$. Note that $m \equiv 0 \pmod p$ iff $n \equiv 0 \pmod p$ and in both cases we'd get $m^2 + mn + n^2 = p$ would have to be divisible by p^2 which is impossible. So let's suppose $n \not\equiv 0 \pmod p$. We'd get that $m^3 - n^3 = (m-n)(m^2 + mn + n^2) \equiv 0 \pmod p$ and so $(m/n)^3 \equiv 1 \pmod p$. But in $\mathbb{F}_p^\times$, a group of order $p - 1 \equiv 1 \pmod 3$ the order of m/n must divide both 3 and $p - 1$ and so it has to be 1, yielding $m \equiv n \pmod p$. But then $m^2 + mn + n^2 \equiv 3n^2 \equiv 0 \pmod p$ which is impossible as $p \neq 3$ and $p \nmid n$.

Alternatively $m^2 + mn + n^2 = p$ after completing the square becomes $(m + n/2)^2 + 3n^2/4 = p$ and the LHS mod 3 is 0 or 1 while the RHS is 2.

(d): Let g be a generator of $\mathbb{F}_p^\times$, of order $p - 1 = 3k$ for some k. Then $x = g^k$ has order 3 and so $x^3 - 1 \equiv 0 \pmod p$. So $p \mid x^3 - 1 = (x-1)(x^2 + x + 1)$ and since $x = g^k \not\equiv 1 \pmod p$ we get $p \mid x^2 + x + 1$.

(d): Factor p in $\mathbb{Z}[\zeta]$. As in the case of $\mathbb{Z}[i]$, we may write $p = up_1 \cdots p_r q_1 \overline{q}_1 \cdots q_s \overline{q}_s$ where u is a unit, $p_1, \ldots, p_r$ are primes of $\mathbb{Z}[\zeta]$ which happen to be in $\mathbb{Z}$ and q_i are primes of $\mathbb{Z}[\zeta]$ which are not real numbers. Then

$$|p|^2 = p^2 = \prod p_i^2 \prod |q_j|^4$$

so either $r = 1, s = 0$ and p is a prime in $\mathbb{Z}[\zeta]$ or $r = 0, s = 1$ and $p = q\overline{q}$ where q is a prime of $\mathbb{Z}[\zeta]$. If not the latter then p would have to be prime in $\mathbb{Z}[\zeta]$.

But part (d) gives $p \mid x^2 + x + 1 = (x - \zeta)(x - \zeta^2)$ and if p were prime in $\mathbb{Z}[\zeta]$ then $p \mid x - \zeta$ or $p \mid x - \zeta^2$. Then either $x - \zeta$ or $x - \zeta^2$ would be of the form $p(a + b\zeta) = pa + pb\zeta$ which cannot be as $p \nmid 1$. $\square$