Math 30810 Honors Algebra 3
Homework 12

Andrei Jorza

Due at noon on Thursday, December 1

Do 8 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) Artin 11.6.8 (a), (b) on page 356.

   Proof. (a): Let $i + j = 1$ for $i \in I$ and $j \in J$. If $x \in I \cap J$ then $xi \in IJ$ and $xj \in IJ$ and so $xi + xj = x \in IJ$. This means $I \cap J \subset IJ$ and the reverse inclusion I did in class.

   (b): Define $f : R/IJ \to R/I \times R/J$ by $f(r \mod IJ) = (r \mod I, r \mod J)$. This is a ring homomorphism. If $f(r \mod IJ) = (0, 0)$ then $r \in I$ and $r \in J$ so $r \in I \cap J = IJ$ so $r \mod IJ = 0$ which means f is injective. If $a \in R/I$ and $b \in R/J$ denote by a and b as well some representatives of these cosets in R. Then define $x = aj + bi \mod IJ$ with i and j from (a). Since $i + j = 1$ it follows that $aj + bi \equiv a \pmod I$ and $\equiv b \pmod I$ and so f is also surjective with $f(x) = (a, b)$. □

2. (You have to do this problem) Let R be a ring and I an ideal of $R[X]$. For a polynomial $P(X) \in R[X]$ let $\ell(P)$ be the leading coefficient of $P(X)$. Define $J = \{\ell(P) \mid P \in I\}$. Show that J is an ideal of R. (This is very useful.)

   Proof. If $a, b \in J$ let $P, Q \in I$ such that $a = \ell(P)$ and $b = \ell(Q)$. Suppose P has degree m and Q has degree n. Then $X^nP(X) + X^mQ(X)$ has degree $m + n$ and has leading term $a + b$. Since $X^nP + X^mQ \in I$ it follows that $a + b \in J$. Now if $a \in I$ with $a = \ell(P)$ and $r \in R$ then clearly $ar = \ell(rP)$. As $P \in I$ it follows that $rP \in I$ and so $ar \in J$. □

3. Consider the ring $R = \mathbb{Z}[\sqrt{-14}] = \{m + n\sqrt{-14} \mid m, n \in \mathbb{Z}\}$. Let $I = (3, 1 + \sqrt{-14})$. Show that $I^2 = (9, 7 + \sqrt{-14})$ and that $I^4 = (5 + 2\sqrt{-14})$ and thus that I^4 is a principal ideal. (One can, in fact, show that the fourth power of any ideal in this ring is principal, but this would be the topic of a graduate number theory course.)

   Proof. Write $a = \sqrt{-14}$. Then $I = (3, 1 + a)$ and so

   $$I^2 = (9, 3 + 3a, 2a - 13) = (9, 3 + 3a, a + 16) = (9, 7 + a, 3 + 3a)$$

   Since $3 + 3a = 3(7 + a) - 2 \cdot 9$ it follows that $I^2 = (9, 7 + a)$. Next

   $$I^4 = (9, 7 + a)^2 = (81, 63 + 9a, 35 + 14a)$$

   Note that $2 \cdot 14 - 3 \cdot 9 = 1$ so I^4 also contains $2(35 + 14a) - 3(63 + 9a) + 2 \cdot 81 = 43 + a$. But since $14a + 35 = 5(43 + a) + 63 + 9a - 3 \cdot 81$ it follows that

   $$I^4 = (81, 63 + 9a, 43 + a)$$

and since $63 + 9a = 9(43 + a) - 4 \cdot 81$ we deduce that $I^4 = (81, 43 + a)$. We need to show that $I^4 = (5 + 2a)$. We compute $\frac{81}{5+2a} = \frac{81(5-2a)}{81} = 5 - 2a$ and $\frac{43+a}{5+2a} = \frac{(43+a)(5-2a)}{81} = 3 - a$ so we deduce that $I^4 \subset (5 + 2a)$. But $5 + 2a = 2(43 + a) - 81$ and so $I^4 = (5 + 2a)$. □

4. Artin 11.3.3 on page 354

   Proof. (a): The kernel consists of polynomials with no constant coefficients so polynomials in the ideal (X, Y).

   (b): If $P \in \mathbb{R}[X]$ and $P(2 + i) = 0$ then $P(2 - i) = 0$ as well so $P(X)$ is divisible by $(X - (2 + i))(X - (2 - i)) = X^2 - 4X + 5$ which is irreducible. Thus the kernel is $(X^2 - 4X + 5)$.

   (c): Suppose $P \in \mathbb{Z}[X]$ has root $1 + \sqrt{2}$. Note that $Q(X) = (X - 1)^2 - 2 = X^2 - 2X - 1$ also has root $1 + \sqrt{2}$ and that Q is irreducible in $\mathbb{Q}[X]$. Look at the ideal (Q, P) in $\mathbb{Q}[X]$. This ideal is not $\mathbb{Q}[X]$ as otherwise $QA + PB = 1$ for some A, B but the LHS vanishes as $1 + \sqrt{2}$. Thus $(Q, P) = (D)$ for some polynomial D. Since Q is irreducible we deduce that $D = Q$ and so $Q \mid P$ in $\mathbb{Q}[X]$. From class, since Q is monic, we can divide with remainder in $\mathbb{Z}[X]$ to get $P(X) = Q(X)A(B) + R(X)$ with R of degree $< \deg Q = 2$. But then $R(1 + \sqrt{(2)}) = 0$ and so R cannot be of degree < 2 in $\mathbb{Z}[X]$ and so $Q \mid P$ in $\mathbb{Z}[X]$. The kernel is therefore (Q).

   (d): Again $Q(X) = X^4 - 10X^2 + 1$ has $\sqrt{2} + \sqrt{3}$ as a root. Its roots are $\pm\sqrt{2} \pm \sqrt{3}$ so Q has no linear factor over $\mathbb{Q}[X]$. If Q we reducible over $\mathbb{Q}[X]$ it would be a product of quadratics $(X^2 + aX + b)(X^2 + cX + d)$. But then $a + c = 0$, $b + ac + d = 10$, $bc + ad = 0$ and $bd = 1$. We deduce that $c = -a$, then from the third equation either $a = 0$ or $b = d$. If $a = c = 0$ then $Q(X) = (X^2 + b)(X^2 + d)$ but solving the quadratic $Y^2 + 10Y + 1 = 0$ with $Y = X^2$ yields irrational roots $-b, -d$. If $a, c \neq 0$ then $b = d$. Then $b = d = \pm 1$ and $2b - a^2 = 10$. In all cases we get a irrational. Thus $Q(X)$ is irreducible and as in part (c) we get $(Q(X))$ is the kernel.

   (e): Clearly $y - x^2$ and $z - x^3$ lie in the kernel. I claim that in fact they generate the kernel. Suppose $P(x, y, z)$ is a polynomial such that $P(x, x^2, x^3) = 0$ as a polynomial. Consider $R(z) = P(x, x^2, z) \in \mathbb{C}[x][z]$. Since $R(x^3) = 0$ it follows that $R(z) = P(x, x^2, z) = (z - x^3)A(x, z)$ for some polynomial A.

   Now look at $Q(y) = P(x, y, z) - P(x, x^2, z) \in \mathbb{C}[x, z][y]$. Since $Q(x^2) = 0$ it follows that $Q(y) = P(x, y, z) - P(x, x^2, z) = (y - x^2)B(x, y, z)$ for some polynomial B. We deduce that $P \in (y - x^2, z - x^3)$. □

5. Artin 11.3.4 on page 355.

   Proof. Clearly $y + 1 - (x - 1)^3$ is in the kernel. Now if $Q(y) = P(x, y)$ is such that $P(x, (x - 1)^3 - 1) = 0$ it follows that $Q(y) = (y + 1 - (x - 1)^3)A(x, y)$ and so the kernel is the principal ideal $(y + 1 - (x - 1)^3)$.

   Now suppose that I is any ideal that contains the kernel. The correspondence theorem says that I is uniquely determined by $I/\ker$ which is an ideal of $\mathbb{C}[x, y]/\ker \cong \mathbb{C}[x]$.

   Every ideal of $\mathbb{C}[x]$ is principal (from class) and so $I/\ker = (a)$ for some polynomial a. But then $I = \ker + (a)$ is now generated by 2 elements as desired. □

6. Artin 11.3.9 on page 355.

   Proof. (a): If $x^n = 0$ then $(1 + x)(1 - x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1}) = 1 + (-1)^n x^n = 1$ so $1 + x$ is invertible.

   (b): For some large enough n, $a^{p^n} = 0$ as a is nilpotent. Then $(1 + a)^{p^n} = 1 + a^{p^n} = 1$. We know from class that $x \mapsto x^p$ is a ring homomorphism which is why we could do this computation. □

7. Artin 11.3.10 on page 355.

Proof. From class every ideal is principal of the form $(f(t))$. Write $f(t) = t^n g(t)$ where $g(0) \neq 0$. Then g is invertible in $F[\![t]\!]$ and so $(f(t)) = (t^n)$. Therefore the ideals of $F[\![t]\!]$ are all of the form (t^n) for $n \geq 0$ as well as (0). □

8. Artin 11.4.4 on page 355.

   Proof. Suppose $f : \mathbb{Z}[x]/(2x^2+7) \to \mathbb{Z}[x]/(x^2+7)$ is a ring isomorphism. Then $0 = f(0) = f(2x^2+7) = 2f(x)^2 + 7$ and so $2f(x)^2 + 7$ must be divisible by $x^2 + 7$ in $\mathbb{Z}[x]$ which means that the polynomial $2f(x)^2 + 7$ must vanish as $\sqrt{-7}$. But then $f(x)$ evaluated at $\sqrt{-7}$ is of the form $a + b\sqrt{-7}$ for rationals a, b and we'd have $2(a + b\sqrt{-7})^2 + 7 = 0$. Opening parentheses we see that $ab = 0$ and in both cases we get a contradiction. So the rings are not isomorphic. □

9. Artin 11.6.7 on page 356.

   Proof. If $P(X)$ is divisible by 2 and X in $\mathbb{Z}[X]$ then $P(X) = XQ(X)$ and $Q(X)$ must have even coefficients. Thus $2X \mid P(X)$. We conclude that $(2) \cap (X) = (2X)$. Consider the map $\phi : \mathbb{Z}[X] \to \mathbb{F}_2[X] \times \mathbb{Z}$ defined by $\phi(P(X)) = (P(X) \mod 2, P(0))$. This is clearly a ring homomorphism. Its kernel consists of $P(X)$ such that $P(X)$ is even (so (2)) and $P(0) = 0$ (so (X)). Thus the kernel is $(2) \cap (X) = (2X)$. We deduce that $\mathbb{Z}[X]/(2X) \cong \operatorname{Im}\phi$. By construction $\operatorname{Im}\phi$ is contained in the desired subring. If $Q(X) \in \mathbb{F}_2[X]$ and $n \in \mathbb{Z}$ are such that $n \equiv Q(0) \pmod 2$ then pick any lift $R(X)$ of $Q(X)$ to $\mathbb{Z}[X]$ and define $P(X) = Q(X) - Q(0) + n$. Then $\phi(R(X)) = (Q(X), n)$ so $\operatorname{Im}\phi$ is exactly the desired subring. □

10. Artin 11.M.7 on page 358.

    Proof. (a): Following the hint if $f_1, \ldots, f_n$ have no common zero then $g = \sum f_i^2 \in I$ has no zeros and therefore the function $1/g$ is continuous and well-defined. This means that g is invertible and so I must be the unit ideal.

    (b): If $a \in [0, 1]$ then $\mathfrak{m}_a = \{f : [0, 1] \to \mathbb{R} \mid f(a) = 0\}$ is an ideal of R (from class). I claim that $\mathfrak{m}_a$ is a maximal ideal. Pick any $0 \neq f \in R/\mathfrak{m}_a$ and denote by f any representative in R. By assumption $f \notin \mathfrak{m}_a$. We need to show that f is invertible in $R/\mathfrak{m}_a$, which then implies that $R/\mathfrak{m}_a$ is a field. By continuity there exists an open neighborhood of a in $[0, 1]$ in which f doesn't vanish and, shrinking this neighborhood, we find a closed neighborhood $[c, d]$ of a on which f is nonzero. Define $g \in R$ by

    $$g(x) = \begin{cases} \frac{1}{f(x)} & x \in [c, d] \\ \frac{1}{f(c)} & x \leq c \\ \frac{1}{f(d)} & x \geq d \end{cases}$$

    Clearly g is continuous and well-defined and $fg - 1 \in \mathfrak{m}_a$. Thus f is invertible mod $\mathfrak{m}_a$.

    Now suppose that $\mathfrak{m}$ is any maximal ideal of R. We need to show that $\mathfrak{m} = \mathfrak{m}_a$ for some a. Suppose that the functions in $\mathfrak{m}$ have no common root. That means that for each $a \in [0, 1]$ there exists a function $f_a \in R$ such that $f_a(a) \neq 0$. By continuity there exists an open neighborhood U_a of a such that $0 \notin f_a(U_a)$. Then $[0, 1]$ is covered by the opens $\{U_a \mid a \in [0, 1]\}$ and compactness of $[0, 1]$ implies that finitely many suffice. Let $U_{a_1} \cup \ldots \cup U_{a_n} = [0, 1]$. This means that every $a \in [0, 1]$ is in some U_{a_i} and thus $f_i(a) \neq 0$. But this would imply that $\{f_{a_1}, \ldots, f_{a_n}\}$ have no common root which would imply that $\mathfrak{m}$ is the unit ideal, contradicting the definition of maximality. We conclude that for some $a \in [0, 1]$, every function $f \in \mathfrak{m}$ vanishes as a. Immediately $\mathfrak{m} \subset \mathfrak{m}_a$ and maximality of $\mathfrak{m}$ implies that $\mathfrak{m} = \mathfrak{m}_a$ as an ideal is maximal if it is maximal with respect to inclusion.

    □