Math 123 Problem set 5

Artin 11.4.7 Factor the following polynomials into irreducible factors in \( \mathbb{Q}[x] \):

(a) \( x^3 - 3x - 2 \)
(b) \( x^3 - 3x + 2 \)
(c) \( x^9 - 6x^6 + 9x^3 - 3 \)

Solution: The first two polynomials are cubes, so if they factor, they have a root; and they are monic, which means that the root over \( \mathbb{Q} \) must be an integer.

Recall that the numerator of the root (if any) must divide the constant term \(-2\), so we must test \( \pm 1, \pm 2 \). We observe that 2 and \(-1\) are both roots: \( x^3 - 3x - 2 = (x - 2)(x + 1)^2 \).

(b) Here, 1 and \(-2\) are both roots: \( x^3 - 3x + 2 = (x + 2)(x - 1)^2 \). Note that this polynomial is \(-f(-x)\), where \( f \) is the polynomial of part (a).

(c) This is an Eisenstein polynomial for the prime 3, hence irreducible.

Artin 11.4.8 Let \( p \) be a prime integer. Prove that the polynomial \( x^n - p \) is irreducible in \( \mathbb{Q}[x] \).

Solution: If \( n = 1 \) this is trivially true (it’s linear), so we’ll focus on \( n > 1 \). Let \( f(x) = x^n - p \), then

\[
f(x + p) = (x + p)^n - p = x^n + \binom{n}{1} x^{n-1} p + \ldots + \binom{n}{n-1} x p^{n-1} + (p^n - p)
\]

Now, this is a monic polynomial, all the non-leading coefficients are divisible by \( p \), and the constant term \( p^n - p \) is not divisible by \( p^2 \) (since \( p^2 | p^n \), but \( p^2 \nmid p \)): by the Eisenstein criterion, \( f(x + p) \) is irreducible. On the other hand, if we had \( f(x) = g(x) h(x) \) then \( f(x + p) = g(x + p) h(x + p) \): that is, if \( f(x + p) \) is irreducible, so is \( f(x) \).

Artin 11.4.16 Let \( f(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \) be a monic polynomial with integer coefficients, and let \( r \in \mathbb{Q} \) be a rational root of \( f(x) \). Prove that \( r \) is an integer.

Solution: Didn’t we do this in class? Suppose \( q \) is the denominator of \( r \), that is, \( r = p/q \) in lowest terms. Then \( q^{n-1}(f(r) - r^n) \) is an integer, but \( q^{n-1}r^n \) has \( q \) in the denominator; therefore, their sum is not an integer, and cannot be zero.

Artin 11.5.3 Factor the following into Gauss primes.

(a) \( 1 - 3i \)
(b) \( 10 \)
(c) \( 6 + 9i \)

Solution: (a) \( 1 + 3i \) has norm 10, which factors as \( 2 \times 5 = (1 + i)(1 - i) \times (1 + 2i)(1 - 2i) \). We have \( 1 + 3i = (1 + i)(2 + i) \).

(b) \( 10 = 2 \times 5 = i(1 + i)^2(1 + 2i)(1 - 2i) \). Note that all these elements have prime norms, and \( 1 + 2i \) and \( 1 - 2i \) are not associates (their ratio in \( \mathbb{C} \) is \(-2/5 + 4/5i \), which is not a Gaussian integer).

(c) \( 6 + 9i = 3(2 + 3i) \). 3 stays prime because it’s a rational prime congruent to 3 modulo 4; and \( 2 + 3i \) has norm 13 (prime in \( \mathbb{Z} \)), so is a prime.

Artin 11.5.5 Let \( \pi \) be a Gauss prime. Prove that \( \pi \) and \( \overline{\pi} \) are associate if and only if either \( \pi \) is associate to an integer prime or \( \pi \overline{\pi} = 2 \).

Solution: “Only if” is easy: if \( \pi = n \) or \( \pi = in \) for \( n \in \mathbb{Z} \) then \( \overline{\pi} = \pm \pi \); and if \( \pi \overline{\pi} = 2 \) then \( \pi \) (and \( \overline{\pi} \)) are associate to \( 1 + i \) (note that \( 1 - i = (-i)(1 + i) \)).

Conversely, suppose \( \pi \) and \( \overline{\pi} \) are associate. If \( \pi = \overline{\pi} \) then \( \pi \in \mathbb{Z} \); and if \( \pi = -\overline{\pi} \) then \( \pi \in i\mathbb{Z} \) (if \( \pi = a + bi \) and \( \overline{\pi} = a - bi \), we must have \( a = 0 \) for \( \overline{\pi} = -\pi \)). It remains to check when \( \overline{\pi} = \pm i\pi \). If \( \pi = a + bi \), \( \overline{\pi} = a - bi \) then to have \( \overline{\pi} = i\pi \) we must have \( a = -b \); to have \( \overline{\pi} = -i\pi \) we must have \( a = b \). Now the only way for \( \pi \) to be prime with such coefficients is if \( a = \pm b = \pm 1 \); in which case we get the primes of norm 2.
Artin 11.5.8 Let $R$ be the ring $\mathbb{Z}[\sqrt{3}]$. Prove that a prime integer $p$ is a prime element of $R$ if and only if the polynomial $x^2 - 3$ is irreducible in $\mathbb{F}_p[x]$.

Solution: $p$ is a prime element of $R$ iff $R/(p)$ is a domain. Now, $R \cong \mathbb{Z}[x]/(x^2 - 3)$, so

$$R/(p) \cong \mathbb{Z}[x]/(x^2 - 3, p) \cong \mathbb{Z}/(p)[x]/(x^2 - 3) \cong \mathbb{F}_p[x]/(x^2 - 3).$$

This quotient is a domain iff $(x^2 - 3)$ is a prime ideal of $\mathbb{F}_p[x]$, i.e. iff $x^2 - 3$ is irreducible.

Artin 11.5.8 Let $R = \mathbb{Z}[\zeta]$, where $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$ is a complex cube root of 1. Let $\rho$ be an integer prime $\neq 3$. Adapt the proof of Theorem (5.1) to prove the following:

(a) The polynomial $x^2 + x + 1$ has a root in $\mathbb{F}_p$ if and only if $p \equiv 1 \mod 3$.

(b) $(p)$ is a prime ideal of $R$ if and only if $p \equiv -1 \mod 3$.

(c) $p$ factors in $R$ if and only if it can be written in the form $p = a^2 + ab + b^2$, for some integers $a, b$.

(d) Make a drawing showing the primes of absolute value $\leq 10$ in $R$.

Solution: (a) Note that $x^2 + x + 1 = \frac{x^3 - 1}{x - 1}$, so the statement is equivalent to showing that $x^3 - 1$ has roots other than 1 iff $p \equiv 1 \mod 3$. Recall that $\mathbb{F}_p^\times$ is a group under multiplication. Now, if there is an element of order 3 in $\mathbb{F}_p^\times$, then $3|\mathbb{F}_p^\times| = p - 1$, so $p \equiv 1 \mod 3$. To show the converse, suppose $p \equiv 1 \mod 3$, so that $p|\mathbb{F}_p[\text{times}]$. If we wish to follow Artin, we now consider the Sylow-3 subgroup of $\mathbb{F}_p^\times$, which has order $3^k$ for some $k \geq 1$; any nonidentity element $g$ of this group has order $3^d$, say, and therefore $g^{3d-1}$ has order 3 as required. We could also use the fundamental theorem of abelian groups to find a subgroup of order $3^k$.

Alternatively, we could follow the same method as for squares: consider the polynomial $x^{\frac{p-1}{3}} - 1$. Note that all cubes solve it; therefore, there are no more than $\frac{p-1}{3}$ distinct cubes in $\mathbb{F}_p^\times$, and in particular there are some distinct elements $g, h \in \mathbb{F}_p^\times$ such that $g^3 = h^3$. Then $(g/h)^3 = 1$ but $g/h \neq 1$.

(b) Since we aren’t considering $p = 3$, all primes are either 1 or $-1$ modulo 3. Now, $(p)$ is a prime ideal of $R$ iff $R/(p)$ is a domain. We have

$$R \cong \mathbb{Z}[x]/(x^2 + x + 1)$$

since $x^2 + x + 1$ is a monic irreducible polynomial that $\zeta$ satisfies. Then

$$R/(p) \cong \mathbb{Z}/(p)[x]/(x^2 + x + 1) \cong \mathbb{F}_p[x]/(x^2 + x + 1),$$

and we just showed that $x^2 + x + 1$ is irreducible over $\mathbb{F}_p$ iff $p \equiv -1 \mod 3$; therefore, $(x^2 + x + 1)$ is a prime ideal and $R/(p)$ a domain iff $p \equiv -1 \mod 3$.

(c) We have the norm function in $R$: $\|a + b\zeta\| = (a + b\zeta)(a + b\zeta) = (a + b\zeta)(a + b\zeta^2) = a^2 - ab + b^2$. This norm is multiplicative (since $\|\alpha\| = \alpha\overline{\alpha}$ in $\mathbb{C}$) and a non-negative integer (integer since $a^2 + ab + b^2$, nonnegative because it’s a $\mathbb{C}$-norm, or because $a^2 + ab + b^2 = (a + b/2)^2 + 3/2b^2$).

Now, suppose $p = \alpha\beta$ in $R$; then $\|p\| = \|\alpha\||\beta\|$, or $p^2 = \|\alpha\|^2\|\beta\|$. Now if $\|\alpha\| = 1$ then $\alpha\overline{\alpha} = 1$, so $\alpha$ is clearly a unit; this is not a satisfactory factorization, so for a nontrivial factorization of $p$ we must have $\|\alpha\| = \|\beta\| = p$, or $p = a^2 + ab + b^2$ (if $\alpha = a + b\zeta$). Conversely, if $p = a^2 + ab + b^2$ then $p = (a + b\zeta)(a + b\zeta^2) = (a + b\zeta)(a + b(-1 - \zeta))$. 
(d) Note that primes in $R$ have norms that are either $p \in \mathbb{Z}$ (if $p \equiv 1 \text{ mod } 3$) or $p^2 \in \mathbb{Z}$ (if $p \equiv -1 \text{ mod } 3$); also, the element $\sqrt{-3}$ (and its associates) has norm 3. Indeed, first I claim that $\pi$ and $\bar{\pi}$ are not associates unless $\pi$ is associate to an integer; note that the units in $R$ are the sixth roots of unity (this is easily checked, since the norm of a unit must be 1).

If $\pi = \bar{\pi}$ then $\pi \in \mathbb{Z}$. Let $\pi = a + b\zeta$, and $\bar{\pi} = a - b\zeta$. Now,

$$\pi(1 - \zeta) = e^{2\pi i/6}\pi = a + b\zeta - a\zeta - b\zeta^2 = (a + b) + (2b - a)\zeta$$

isn’t equal to $\bar{\pi}$ since we can’t have $a = b = 0$;

$$\pi(1 - \zeta)^2 = \pi\zeta = a\zeta + b(-1 - \zeta) = -b + (a - b)\zeta$$

which would again mean $a = b = 0$;

$$\pi(1 - \zeta)^3 = -\pi = -a - b\zeta$$

implies $a = 0$, so $\pi = p\zeta$ is associate to an integer;

$$\pi(1 - \zeta)^4 = -\pi(1 - \zeta) = (-a - b) + (a - 2b)\zeta$$

implies $-b = a - 2b$ so $a = b$, but $a = -a - b$ so $a = b = 0$;

$$\pi(1 - \zeta)^5 = -\pi\zeta = b + (b - a)\zeta$$

would mean $a = b = 0$ once more.

Thus, by an exhaustive check we’ve shown that $\pi$ and $\bar{\pi}$ aren’t associates, and are therefore relatively prime, unless they are associate to an integer. We conclude that the norm of $\pi$ must be a rational prime unless $\pi$ is associate to an integer, since if $p\|\pi\|$ then $\pi|p$ or $\bar{\pi}|p$, but if one of those holds then so does the other (conjugate the division), and (since $\pi$, $\bar{\pi}$ are relatively prime) we conclude $\pi\bar{\pi}|p$: that is, $\|\pi\|\|p\|$, so $\|\pi\| = p$.

We are finally ready to tackle the primes in $R$ of absolute value $\leq 10$.

The rational primes in that range that stay prime are 2 and 5; the rational prime 3 splits as $3 = -\sqrt{-3}$.

Now for the primes $\equiv 1 \text{ mod } 3$, which are norms of elements: note that that if $p = a^2 + a + 1$ then $p - 1 = a(a + 1)$; this is not hard to spot. Also, it’s worth noting that at least one of $a$ and $b$ must be odd.

$7 = 2^2 + 2 \times 1 + 1^2 = \|2 - \zeta\|
13 = 3^2 + 3 \times 1 + 1^2 = \|3 - \zeta\|
19 = 3^2 + 3 \times 2 + 2^2 = \|3 - 2\zeta\|
31 = 5^2 + 5 \times 1 + 1^2 = \|5 - \zeta\|
37 = 3^2 + 3 \times 4 + 4^2 = \|3 - 4\zeta\|
43 = 6^2 + 6 \times 1 + 1^2 = \|6 - \zeta\|
61 = 5^2 + 5 \times 4 + 4^2 = \|5 - 4\zeta\|
67 = 7^2 + 7 \times 2 + 2^2 = \|7 - 2\zeta\|
73 = 8^2 + 8 \times 1 + 1^2 = \|8 - \zeta\|
79 = 7^2 + 7 \times 3 + 3^2 = \|7 - 3\zeta\|
97 = 8^2 + 8 \times 3 + 3^2 = \|8 - 3\zeta\|

Each of these gets 6 associates from the 6 units, plus 6 more associates for its conjugate (which isn’t associate to the prime!).
**Text problem** In the following exercises we prove the following statement that we claimed in class: the polynomial $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$, but its image in $\mathbb{F}_p[x]$ is reducible for every $p$.

- Let $a, b \in \mathbb{Z}$. Prove that, for every prime integer $p$, the polynomial $P(x) = x^4 + ax^2 + b^2$ is reducible, by following the following hints:
  
  (a) First, prove the statement for $p = 2$, and from now on we assume that $p \neq 2$.
  
  (b) Consider the map $\rho : \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$ given by $x \mapsto x^2$. Show that the image of $\rho$ contains precisely $\frac{p-1}{2}$ elements. We call the elements in the image of $\rho$ the *quadratic residues* modulo $p$, and the elements which are not in the image of $\rho$ quadratic non-residues.
  
  (c) Show that the quadratic non-residues are precisely the elements $x \in \mathbb{F}_p^*$ such that $x^{\frac{p-1}{2}} = -1$. In particular, show that the product of two quadratic non-residues is a quadratic residue.

- Let $s$ be an integer such that $a \equiv 2s \mod p$. Show that

  \[
  P(x) = (x^2 + s)^2 - (s^2 - b^2) = (x^2 + b)^2 - (2b - 2s)x^2 = (x^2 - b)^2 - (-2b - 2s)x^2.
  \]

  (e) Deduce that $P(x)$ is reducible in $\mathbb{F}_p[x]$.

- Prove that $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$.

**Solution:**

- (a) Every even polynomial over $\mathbb{F}_2$ is a square, since squaring is a ring homomorphism in characteristic 2, and all constants are squares. Thus $x^4 + ax^2 + b^2$ is always a square, hence reducible.

- (b) Note $x \neq -x$ for $p \neq 2$, but $x^2 = (-x)^2$. Therefore, the image of $\rho$ contains no more than $\frac{p-1}{2}$ elements. On the other hand, every $a \in (\mathbb{F}_p^*)^2$ has no more than two square roots, since the equation $x^2 = a$ has at most two solutions. Consequently, there are at least $\frac{p-1}{2}$ squares, hence exactly that many.
(c) Note that for every $x$ we have $x^{p-1} = 1$, so $x^{p-1}/2 = \pm 1$ (recall that we have exactly two square roots of 1). Now, if $x = a^2$ then $x^{p-1}/2 = a^{p-1} = 1$; and as we showed above, there are $\frac{p-1}{2}$ squares. Since the equation $x^{p-1}/2 = 1$ can have no more than $\frac{p-1}{2}$ solutions, the non-residues don’t get to solve it: so the non-residues must have $x^{p-1}/2 = -1$.

Now, if I get two non-residues $x$ and $y$, then $x^{p-1}/2 = y^{p-1}/2 = -1$, so $(xy)^{p-1}/2 = 1$, and $xy$ is a residue.

(d) The algebraic computation proper is boring; it works. (No, you aren’t allowed to claim this on your solutions!) It’s worth noticing that $s^2 - b^2 = (s + b)(s - b) = \frac{1}{4}(2b - 2s)(-2b - 2s)$.

(e) As the remark above points out, one of the three lines factors as a difference of two squares: that is, if $2b - 2s$ and $-2b - 2s$ are both not squares, then the first line must factor as a difference of two squares. (If either of them is a square, that particular line factors as the difference of squares.)

- Suppose $x^4 + 1 = fg$ for $f$, $g$ nonconstant polynomials. First, note that $x^4 + 1$ has no roots in $\mathbb{R}$ (since $x^4 > 0$), and therefore has no linear factors: therefore, $f$ and $g$ must both have degree 2. Let $f = ax^2 + bx + c$ and $g = a'x^2 + b'x + c'$, then

$$fg = aa'x^4 + (ab' + a'b)x^3 + (ac' + a'c + bb')x^2 + (bc' + b'c)x + cc'$$

Recall that our factorization must be over $\mathbb{Z}$, so from $aa' = 1$ we conclude that $a = a' = \pm 1$; WLOG we may flip the two signs and assume $a = a' = 1$. Now for the constant term we also get $cc' = 1$, so also $c = c' = \pm 1$. However, in degree 3 we get $b + b' = 0 \implies b = -b'$; and in degree 2 we therefore get $c + c' - b^2 = 0$, or $c + c' = b^2$. However, $c + c' = \pm 2$ is not a square in $\mathbb{Z}$, so the polynomial does not in fact factor.