Solution Set 2

Math 123
February 20, 2002

1. *Artin §11.3 #8*

Let $R = \mathbf{C}[y, z, w]$, so we want to show that $f(x) = xw - yz$ is irreducible in $R[x]$. Since $\gcd(w, yz) = 1$ (the prime factorization of yz is $y \cdot z$), f is irreducible, so by Artin Prop. 11.3.6, since f is irreducible in $\mathbf{C}(y, z, w)(x)$ (it is linear), f is irreducible in R.

---

2. *Artin §11.4 #1*[1]

a) We have $f(x) = x^2 + 27x + 213 \equiv x^2 + x + 1 \pmod 2$; since the latter is irreducible in $\mathbf{F}_2[x]$ ($f(0) = f(1) = 1$), f is irreducible in $\mathbf{Q}[x]$.

b) Since 3 does not divide 1, $3|6$ and 12, and 9 does not divide 12, by Eisenstein's Criterion, $x^3 + 6x + 12$ is irreducible in $\mathbf{Q}[x]$.

c) We have $f(x) = 8x^3 - 6x + 1 \equiv x^3 + x + 1 \pmod 7$. Since f is cubic, if it is not irreducible it has a linear factor and thus a root in $\mathbf{F}_7$. We see by inspection that $f(x) \neq 0$ for all $x \in \mathbf{F}_7$, so f is irreducible.

d) We have $f(x) = x^3 + 6x^2 + 7 \equiv x^3 + x^2 + 2 \pmod 5$. As above, f has no root in $\mathbf{F}_5$, so f is irreducible.

e) This $f(x) = x^5 - 3x^4 + 3$ is irreducible by Eisenstien's criterion with $p = 3$.

---

3. *Artin §11.4 #11*

First we prove the following useful fact.

LEMMA 3.1. *If M is any $n \times n$ complex matrix with $M^k = I_n$ for some k, then M is diagonalizable.*

PROOF.

We will also consider M to be an operator on an n-dimensional complex vector space $V = \mathbf{C}^n$. For vectors $\mathbf{v} = (v_1, \ldots, v_n)$ and $\mathbf{w} = (w_1, \ldots, w_n)$, define $\langle \mathbf{v}, \mathbf{w} \rangle_0 = \bar{v}_1 w_1 + \cdots + \bar{v}_n w_n$ to be the standard complex dot product of $\mathbf{v}$ and $\mathbf{w}$, so $\langle \mathbf{v}, \mathbf{v} \rangle_0 = \sum_{i=1}^n |v_i|^2 =$

[1] Taken from Noam Zeilberger's solutions

$|\mathbf{v}|^2 > 0$. Now let

$$\langle \mathbf{v}, \mathbf{w} \rangle = \sum_{i=0}^{k-1} \langle M^i \mathbf{v}, M^i \mathbf{w} \rangle_0.$$

We claim that $\langle \cdot, \cdot \rangle$ is a positive-definite Hermetian form (see Artin 7.4 and 7.5). Clearly $\langle \cdot, \cdot \rangle$ is a Hermetian form, and for nonzero $\mathbf{v} \in V$,

$$\langle \mathbf{v}, \mathbf{v} \rangle = \sum_{i=0}^{k-1} |M^i \mathbf{v}|^2 > 0.$$

Now, for any $\mathbf{v}, \mathbf{w} \in V$, $\langle M\mathbf{v}, M\mathbf{w} \rangle = \langle \mathbf{v}, \mathbf{w} \rangle$. Thus M is unitary, so $MM^* = I_n = M^*M$, and M is normal. By Artin Theorem 5.4, then, M is diagonalizable.

❐

Let A be as in the problem, and let $c(x) \in \mathbf{Z}[x]$ be the characteristic polynomial of A. Considering A as a complex matrix, find a basis for $V = \mathbf{C}^n$ with respect to which A is diagonal. Since $A \neq I_n$, at least one diagonal entry (eigenvalue) λ is not 1; suppose that $\mathbf{v}$ is a corresponding eigenvector (so $A\mathbf{v} = \lambda\mathbf{v}$). Well, $\mathbf{v} = A^p\mathbf{v} = \lambda^p\mathbf{v}$, so λ is a nontrivial root of $x^p - 1$—that is, λ is a root of the cyclotomic polynomial $f_p(x) = x^{p-1} + \cdots + x + 1$. But since λ is an eigenvalue of A, we have $c(\lambda) = 0$ as well, so since $f_p(x)$ is a primitive irreducible polynomial in $\mathbf{Z}[x]$, f_p divides c, and $n = \deg c \geq p - 1$.

---

4. *Artin §11.4 #12*

As before, we know that any reducible cubic polynomial in $\mathbf{F}_3[x]$ has a root in $\mathbf{F}_3$. Since the arbitrary monic cubic is of the form $f(x) = x^3 + ax^2 + bx + c$, there are 27 such polynomials, but nine of them (the ones with $c = 0$) have a root at 0, so we only have to test eighteen of them. By listing all 18 polynomials and checking each at $x = 0, \pm 1$, we find that the only irreducible ones are $x^3 - x + 1, x^3 - x - 1, x^3 + x^2 - 1, x^3 + x^2 + x - 1, x^3 + x^2 - x + 1, x^3 - x^2 + 1, x^3 - x^2 + x + 1, x^3 - x^2 - x - 1$.

---

5. *Artin §11.5 #3*

Using the criteria for whether a prime in $\mathbf{Z}$ is prime in $\mathbf{Z}[i]$, we can find the prime factorization for an element of $\mathbf{Z}[i]$ by looking at the integer prime factorization of its norm, and trying various combinations of the factors. Thus we can calculate:[2]

a) $(1 - 3i)(1 + 3i) = 10 = 2 \cdot 5 = (1 - i)(1 + i)(1 - 2i)(1 + 2i)$. After some investigation, we obtain $1 - 3i = -(1 + i)(1 + 2i)$.

b) From the previous part, $10 = (1 - i)(1 + i)(1 - 2i)(1 + 2i)$.

[2] From Seth Kleinerman's calculations.

c) We see immediately that $6 + 9i = 3(2 + 3i)$. Well, $(2 + 3i)(2 - 3i) = 13$ which is prime and $3 \not\equiv 1 \pmod 4$, so 3 and $2 + 3i$ are prime in $\mathbf{Z}[i]$ and our factorization is complete.

---

6. *Artin §11.5 #6*

We would like to say that p is prime in $R = \mathbf{Z}[\sqrt{3}]$ if and only if $R/(p)$ is a field. This does *not* follow immediately from by Artin, Proposition 11.2.14 (almost everybody did this wrong)—that proposition only applies to *principal ideal domains* R, and it is not at all obvious that R is a PID. One can prove without too much trouble that R is indeed a PID, but the following is even easier:[3] more or less by definition, p is a prime element if and only if (p) is a prime ideal, which is true if and only if $R/(p)$ is an integral domain, and since $R/(p)$ is clearly finite, this is true if and only if $R/(p)$ is a field (recall that a field is an integral domain and that a finite integral domain is a field).

Now we can proceed as in lecture. We have canonical isomorphisms

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

Since $\mathbf{F}_p[x]$ is a principal ideal domain, we can *now* use Artin Prop. 11.2.14 to conclude that $R/(p)$ is a field if and only if $x^2 - 3$ is irreducible in $\mathbf{F}_p[x]$.

---

7. *Artin §11.6 #3*

We know that if $n \in \mathbf{Q}$ is not square in $\mathbf{Q}$ then $\sqrt{n} \notin \mathbf{Q}$. Suppose that $\sqrt{d'} \in \mathbf{Q}(\sqrt{d})$. Since every element of $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}[x]/(x^2 - d)$ is of the form $a + b\sqrt{d}$ for $a, b \in \mathbf{Q}$, we can write

$$\sqrt{d'} = a + b\sqrt{d} \tag{1}$$

for $a, b \in \mathbf{Q}$. Now, if $a = 0$ then we have $\sqrt{d'/d} = b \in \mathbf{Q}$, which is a contradiction since d'/d is not a square in $\mathbf{Q}$ since d' and d are distinct squarefree integers. So $a \neq 0$, and $b \neq 0$ since $\sqrt{d'}$ is irrational; thus squaring both sides of (1) gives

$$d' = a^2 + b^2 d + 2ab\sqrt{d} \implies \sqrt{d} = \frac{d' - a^2 - b^2 d}{2ab}$$

which is contradiction since $\sqrt{d}$ is irrational as well. Thus $\sqrt{d'} \notin \mathbf{Q}(\sqrt{d})$ and $\mathbf{Q}(\sqrt{d}) \neq \mathbf{Q}(\sqrt{d'})$.

---

8. *Artin §11.6 #7*

Let $R = \mathbf{Z}[\eta]$ be the ring of algebraic integers in $\mathbf{Q}(\sqrt{d})$ for some squarefree integer $d < 0$. We know that $R = \{a + b\eta \mid a, b \in \mathbf{Z}\}$ is a lattice in $\mathbf{C}$ since η is not real; we wish to show that R is maximal, i.e. that there is no strictly larger lattice that is also a subring.

[3] Thanks to Richard Louis Rivero for this one.

Let $S \leq \mathbf{C}$ be a ring containing R that is also a lattice. By Artin Corollary 5.4.15, we can assume that S is generated (as a lattice) by 1 and another element α—there can be no element of S with norm less than 1, since otherwise there would be an infinite number of elements in the unit circle and S would not be a lattice. Since S is a ring, we can write $\alpha^2 = b\alpha + c$ for $b, c \in \mathbf{Z}$, so α is an algebraic integer satisfying $x^2 - bx - c = 0$. Thus $\alpha = \frac{1}{2}(b \pm \sqrt{b^2 - 4c})$, so $\alpha \in \mathbf{Q}(\sqrt{d'})$, where d' is the squarefree part of $b^2 - 4c$. Now, if $d \neq d'$, then since $\sqrt{d} \notin \mathbf{Q}(\sqrt{d'}) \geq S$ by the previous problem, we would have $\sqrt{d} \notin S$ which would contradict the fact that $R \leq S$. Thus $d = d'$ and α is an algebraic integer in $Q(\sqrt{d})$, which means $S = R$, and R is maximal.

---

9. *Artin §11.7 #4*

First we note that for any nonzero $\alpha \in A$, $\alpha\bar{\alpha} \in A$ is a positive integer, so $A \cap \mathbf{Z} \neq 0$. Select the smallest positive integer n in A and apply Artin Corollary 5.4.15 to conclude that there must be a lattice basis for A one of whose elements is n.

---

10. *Artin §11.7 #5*

Let $\delta = \sqrt{-5}$ and let L be the lattice generated by $(3, 1 + \delta)$. By definition, L is an abelian subgroup of R; we must show that $RL = L$. It suffices to show that L is closed under multiplication by δ, and by linearity, all we have to show is that 3δ and $\delta(1+\delta)$ are elements of L. Indeed, $3\delta = 3(1 + \delta) - 3$ and $\delta(1 + \delta) = \delta - 5 = (1 + \delta) - 2 \cdot 3$.

By drawing a picture, one can quickly convince oneself that $\alpha = 1+\delta$ has minimal absolute value in L. Since

$$\frac{1}{2}(\alpha + \alpha\delta) = \frac{1}{2}(2\delta - 4) = \delta - 2 = (\delta + 1) - 3$$

we have $L = (\alpha, \frac{1}{2}(\alpha + \alpha\delta))$ (note that $(\delta + 1) - (\delta - 2) = 3$).

Joe Rabinoff