Math 593 Assignment # 4 Solutions

Bryden R. Cais

October 10, 2002

1. (a) Let $I = \ker \phi \subset \mathbb{Z}$, and let $A \subset R$ denote the image of $\mathbb{Z}$ under ϕ in R. Then we have

$$\mathbb{Z}/I \simeq A.$$

Since $A \subset R$ is an integral domain, I must be a prime ideal of $\mathbb{Z}$. Since the prime ideals of $\mathbb{Z}$ are of the form (0) or (p) for a prime p, we conclude that $A \simeq \mathbb{Z}$ or $A \simeq \mathbb{Z}/(p)$ for some prime p.

(b) Take, for example, $R_p = \mathbb{Z}/(p)[X]$, the ring of polynomials in X with coefficients in $\mathbb{Z}/(p)$. Clearly this is infinite since it is a (countably) infinite dimensional vector space over $\mathbb{Z}/(p)$. Moreover, let $r, s \in R_p$ have degree d, e respectively. Then we can write

$$\begin{aligned} r &= aX^d + \cdots \\ s &= bX^e + \cdots \\ rs &= abX^{d+e} + \cdots, \end{aligned}$$

so that if $rs = 0$ then in particular, $ab = 0 \in \mathbb{Z}/(p)$. Since $\mathbb{Z}/(p)$ is an I.D., we must have a or b equal to 0, which is absurd. Hence R_p is an integral domain.

(c) Let $a \in R$. Then we have

$$p \cdot a = p \cdot 1_R \cdot a = \phi(p) \cdot a.$$

Since R has characteristic p, the image of $\mathbb{Z}$ under ϕ must be $\mathbb{Z}/(p)$, that is, $\phi(p) = 0 \in R$ so we have $p \cdot a = 0 \cdot a = 0$, as required.

(d) It is obvious that F preserves the multiplicative structure of R and that $F(1) = 1, F(0) = F(0)$. So it suffices to check that F is a homomorphism of abelian groups (under the addition of R). Since the binomial theorem holds in any commutative ring, we have

$$F(x + y) = (x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i.$$

It is not difficult to see that $\binom{p}{i}$ is divisible by p for $1 \leq i \leq p - 1$ and therefore, since R has characteristic p, we find that $\binom{p}{i} = 0 \in R$ for $1 \leq i \leq p - 1$ and hence that

$$F(x + y) = x^p + y^p = F(x) + F(y).$$

2. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$$

and suppose that $a_i \in P$, where P is a prime ideal of R, but that $a_0 \notin P^2$. Suppose that f is not irreducible, that is, we have a factorization

$$f = gh.$$

Reducing modulo P gives a factorization

$$\bar{f} = \bar{g}\bar{h}$$

where $\bar{f}, \bar{g}, \bar{h}$ are the images of f, g, h in $R/P[x]$ under the natural quotient map. By hypothesis, we have $\bar{f} = x^n$. Since R/P is an integral domain (P being afterall a prime ideal) it follows that $\bar{g} = x^i, \bar{h} = x^j$ with $i + j = n$ and $0 < i, j$. Writing

$$g = \alpha_i x^i + \cdots + \alpha_0$$
$$h = \beta_j x^j + \cdots + \beta_0,$$

it follows that $\alpha_0, \beta_0 \in P$. By our factorization of f, we must have $a_0 = \alpha_0\beta_0 \in P^2$, a contradiction. Hence f is irreducible.

3. (a) Let p be prime and set

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x].$$

Observe that

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}.$$

Now $\Phi_p(x)$ is irreducible if and only if $\Phi_p(x+1)$ is irreducible. But we have

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} \equiv x^{p-1} \mod p$$

by part d) of question 1. On the other hand, the constant term in $\Phi_p(x+1)$ is clearly

$$\binom{p}{p-1} = p$$

so that $\Phi_p(x+1)$ is irreducible since it is p-Eisenstein.

(b) It is false that for any natural number the polynomial

$$x^{m-1} + \cdots x^{m-2} + \cdots + x + 1$$

is irreducible. A simple counterexample is $m = 4$ when we have

$$x^3 + x^2 + x + 1 = (x+1)(x^2+1).$$

More generally, define

$$\Phi_m(x) = \begin{cases} x - 1 & \text{if } m = 1 \\ \dfrac{x^m - 1}{\prod_{\substack{d \mid m \\ d < m}} \Phi_d(x)} & \text{otherwise} \end{cases}.$$

Then it can be shown that $\Phi_m(x) \in \mathbb{Z}[x]$ is irreducible for every $m > 0$. The polynomial $\Phi_m(x)$ is called the m^{th} *cyclotomic* polynomial.

4. This is a fairly simple counting argument. If a degree two monic polynomial $p(x)$ is reducible, then it splits as the product of two linear factors. By multiplication by a unit if necessary, we can assume that each of these linear factors is monic. Moreover, these monic linear factors are uniquely determined by $p(x)$. To see this, observe that a monic linear polynomial is completely determined by its constant term, and that a, b are uniquely determined by the requirement

$$(x+a)(x+b) = x^2 + cx + d$$

in $\mathbb{F}_p[x]$, since the system of equations $a + b = c, ab = d$ has a unique (up to transposition of a, b) solution (if any) modulo p. It follows that the number of degree 2 reducible polynomials is the same as the number of pairs (where order doesn't matter) of monic linear polynomials. There are

$$\frac{p(p-1)}{2}$$

such pairs if the factors are different, and

$$p$$

pairs if they are the same, for a total of

$$\frac{p(p+1)}{2}$$

reducible degree two monic polynomials. Therefore, there are

$$p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}$$

monic irreducible degree 2 polynomials in $F[x]$.

5. (a) Suppose that $d < 0$ is squarefree and that $a + b\sqrt{d}$ is a unit. Then there exist c, d such that

$$(a + b\sqrt{d})(c + e\sqrt{d}) = 1.$$

Observe that if one of b, e is 0, so is the other, giving the units ± 1. Otherwise, both $b, e \neq 0$. There is a unique, nontrivial automorphism of $\mathbb{Q}[\sqrt{d}]$ fixing $\mathbb{Q}$ pointwise—namely, complex conjugation, which sends $\sqrt{d}$ to $-\sqrt{d}$. Applying this automorphism gives

$$(a + b\sqrt{d})(a - b\sqrt{d})(c + e\sqrt{d})(c - e\sqrt{d}) = (a^2 - db^2)(c^2 - de^2) = 1.$$

Now since $a^2 - db^2, c^2 - de^2 \in \mathbb{Z}$ we have $a^2 - db^2 = \pm 1$. If $d < -1$, this requires $b = 0, a = \pm 1$. If $d = -1$ we can have $a = \pm 1, b = 0$ or $b = \pm 1, a = 0$. The same goes for c, e. In any case, we have determined that the group of units in $\mathbb{Z}[\sqrt{d}]$ is precisely

$$\begin{array}{ll} \{\pm 1\} & \text{if } d \neq -1 \\ \{\pm 1, \pm i\} & \text{if } d = -1 \end{array}$$

(b) Observe that $(\sqrt{2}+1)(\sqrt{2}-1) = 1$ so that $\sqrt{2}-1$ is a unit in $\mathbb{Z}[\sqrt{2}]$. It follows that $(\sqrt{2}+1)^n$ is a unit *for every* $n \in \mathbb{Z}$. Moreover, this gives an infinitude of units as $|\sqrt{2}+1| > 1$ so that $|(\sqrt{2}+1)^n| \neq |(\sqrt{2}+1)^m|$ unless $n = m$. In fact, *every* unit in $\mathbb{Z}\sqrt{2}$ has the form $\pm(1+\sqrt{2})^n$, for some $n \in \mathbb{Z}$ (in other words, the unit group is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}/(2)$).