HOMEWORK 12 (DUE: 11:15 AM, DEC 12 WED)

1. Do Exercise 20.C.1–3 in [Pin10].

   1. Suppose that $a \in A - \{0\}$ is not a unit. Consider the function $\phi : A \to A : x \mapsto ax$. Then it is clearly a homomorphism of abelian groups. Since a is not a unit, $\mathrm{im}\phi \not\ni 1$, which means ϕ is not surjective. Since A is finite, ϕ cannot be injective, thus $\ker\phi \neq \{0\}$. Now choose a nonzero element $b \in \ker\phi$. Then by definition $ab = 0$, thus a is a zero-divisor.

   2. We follow the hint and thus may assume that there exists $n, m \in \mathbb{Z}_{>0}$ such that $n < m$ and $a^n = a^m$. Since a is not a zero-divisor, by part 1 it is a unit, thus we may multiply a^{-n} on both sides. Thus we have $a^{m-n} = 1$. Since $m - n > 0$, we proved the claim.

   3. Let $a^m = 1$ for some $m \in \mathbb{Z}_{>0}$. By replacing m by $2m$ if necessary, we may assume that $m \geq 2$. Then $a^{-1} = a^{m-1}$ and $m - 1 > 0$.

2. Do Exercise 22.B.1–7 in [Pin10]. You are allowed (and even recommended) to use the following fact: for $a, b \in \mathbb{Z}$, we have $(a) + (b) = (\gcd(a, b))$.

   Here we use the following fact: if $(a) + (b) = (c)$ for some $c > 0$, then $\gcd(a, b) = c$.

   1. Since $a|b$, $b \in (a)$, thus $(a) + (b) = (a)$. Thus $\gcd(a, b) = a$ as $a > 0$.

   2. $(a) + (0) = (a)$, thus $\gcd(a, 0) = a$ as $a > 0$.

   3. $(a) + (b + xa) = (a) + (b)$ since $xa \in (a)$. Thus $\gcd(a, b) = \gcd(a, b + xa)$.

   4. Since p is prime, (p) is maximal, thus $(a) + (p)$ equals (p) or $\mathbb{Z} = (1)$. It means $\gcd(a, p)$ equals 1 or p.

   5. By symmetry, it suffices to show that if $\gcd(a, b) | \gcd(c, d)$. But since $\gcd(a, b)$ is a common divisor of a and b, it is a common divisor of c and d, which means $\gcd(a, b) | \gcd(c, d)$.

   6. $(ab) \subset (a)$ and $(ab) \subset (b)$. Thus $(1) = (ab) + (c) \subset (a) + (c)$ and $(1) = (ab) + (c) \subset (b) + (c)$, which means that $\gcd(a, c) = \gcd(b, c) = 1$.

   7. Let $(a') + (b') = (c')$ for some $c' > 0$. Then by multiplying c on both sides, we have $(ca') + (cb') = (cc')$, i.e. $(c) = (a) + (b) = (cc')$. Thus $cc' = c$, i.e. $c' = 1$.

3. Do Exercise 24.A.1–3 (not all) in [Pin10].

1. In $\mathbb{Z}[x]$, $a(x)+b(x) = x^3+7x^2+4x+1, a(x)-b(x) = -x^3-3x^2+2x+1, a(x)b(x) = 2x^5+13x^4+18x^3+8x^2+x$. Thus,

- in $\mathbb{Z}_5[x]$, $a(x)+b(x) = x^3+2x^2+4x+1$, $\quad a(x)-b(x) = 4x^3+2x^2+2x+1$, $\quad a(x)b(x) = 2x^5+3x^4+3x^3+3x^2+x$
- in $\mathbb{Z}_6[x]$, $a(x)+b(x) = x^3+1x^2+4x+1$, $\quad a(x)-b(x) = 5x^3+3x^2+2x+1$, $\quad a(x)b(x) = 2x^5+x^4+2x^2+x$
- in $\mathbb{Z}_7[x]$, $a(x)+b(x) = x^3+4x+1$, $\quad a(x)-b(x) = 6x^3+4x^2+2x+1$, $\quad a(x)b(x) = 2x^5+6x^4+4x^3+x^2+x$

2. $x^3+x^2+x+1 = (x-2)(x^2+3x+2)+(5x+5)$ in $\mathbb{Z}[x]$. Similarly, $x^3+x^2+x+1 = (x+3)(x^2+3x+2)$ in $\mathbb{Z}_5[x]$. (Note that $5x+5=0$ in $\mathbb{Z}_5[x]$.)

3. Indeed, polynomial division in $\mathbb{Z}[x]$ is not well-defined especially when the leading coefficient of the divisor is not a unit, thus it does not make sense to divide x^3+2 by $2x^2+3x+4$. Meanwhile, we have

- in $\mathbb{Z}_3[x]$, $(x^3+2) = (2x)(2x^2+1)+(x+2)$
- in $\mathbb{Z}_5[x]$, $(x^3+2) = (3x+3)(2x^2+3x+4)+(4x)$

(Note that $2x^2+1 = 2x^2+3x+4$ in $\mathbb{Z}_3[x]$.)

4. Do Exercise 25.D.1–7 in [Pin10]. Note that part 3 and 4 were already discussed in the class. For part 1, you need the following definition:

Definition 0.1. For a commutative ring A and its elements $a, b \in A$, a and b are called *associates* to each other if there exists a unit $u \in A$ such that $b = ua$.

Note that $F[x]^\times = F^\times$. It is because for any $f, g \in F[x]$, if $fg = 1$ then $\deg(f) + \deg(g) = \deg(fg) = \deg(1) = 0$, thus $\deg(f) = \deg(g) = 0$.

1. Suppose $(f) = (g)$. Then $g = fx$ and $f = gy$ for some $x, y \in F[x]$. In particular, $f = fxy$. By cancellation law, it means that $xy = 1$, i.e. $x, y \in F^\times$. Thus f and g are associates.

2. For any f generating J, if we let $a \in F^\times$ be the leading coefficient of f then f/a is monic and also a generator of J. Thus such a monic generator of J exists. Now if f and g are two monic generators of J, then f and g are associates by part 1, i.e. there exists $u \in F^\times$ such that $f = gu$. By comparing the leading coefficients, it follows that $u = 1$, thus the monic generator of J is unique. Now if $(m(x)) = J$, then the fact that $a(x) \in J \Leftrightarrow m(x)|a(x)$ is just a reformulation of the definition of an ideal generated by an element.

3. (Here we assume that $J \neq 0$.) Let $(f) = J$. First suppose that J is prime and $f = gh$ for some $g, h \in F[x]$. Then $gh \in J$, thus $g \in J$ or $h \in J$. Without loss of generality we may assume that $g \in J$, i.e. $g = fx$ for some $x \in F[x]$. Then $f = fxh$, thus by cancellation law $xh = 1$, i.e. h is a unit. Thus f is irreducible. Now conversely suppose that f is irreducible. Then for any (g) which properly contains $J = (f)$, i.e. $(f) \subsetneq (g)$, we have $f = gh$, thus either g or h is a unit. If h is a unit, then f and g are associates, thus $(f) = (g)$ which contradicts the assumption. Thus g is a unit, which means $(g) = F[x]$. It means that $J = (f)$ is maximal, thus J is prime.

4. We already proved this in part 3.

5. $S \not\ni 1$, thus $S \neq F[x]$. Also it is trivial that $x - 1 \in S$. Since $(x - 1)$ is maximal by part 4 and $(x - 1) \subset S$, it follows that $(x - 1) = S$.

6. Let $\phi : F[x] \to F$ be a homomorphism such that $\phi(f(x)) = f(1)$. Then it is clearly surjective, and $\ker \phi \ni x - 1$. Also, $\phi(1) \neq 0$, thus $\ker \phi$ is a proper ideal of $F[x]$. Since $S = (x - 1)$ is maximal, it means that $\ker \phi = (x - 1)$. Now the result follows from the fundamental homomorphism theorem.

7. Suppose that $J = (f)$ for some $f \in F[x, y]$. J clearly contains x and y, thus there exists $z, w \in F[x, y]$ such that $fz = x, fw = y$. By considering the degree, f should be expressed as $f = ax + by$ for some $a, b \in F$. But then z and w are all constant, and f is a multiple of both x and y, which is impossible. Thus J is not a principal ideal.

References

[Pin10] Pinter, C. C., *A Book of Abstract Algebra*, 2nd ed., Dover Publications, 2010.