MATH 320 Unit 3 Exercises

Divisibility, plus Unit 1 Revisited

$\mathbb{Z}_p$ Theorem: Let $p \in \mathbb{Z}$ with $p \geq 2$. The following are equivalent: (i) p is prime; (ii) $\mathbb{Z}_p$ is an integral domain; (iii) $\mathbb{Z}_p$ is a field.

$\mathbb{F}[x]$ Division Algorithm Theorem: Let $\mathbb{F}$ be a field, and let $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$. Then there exist unique $q(x), r(x) \in \mathbb{F}[x]$ with $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0_{\mathbb{F}}$ or $deg(r(x)) < deg(g(x))$. We write $(f(x), g(x)) \to DA \to (q(x), r(x))$ or $(f, g) \to DA \to (q, r)$.

Let $\mathbb{F}$ be a field, and let $f(x), g(x) \in \mathbb{F}[x]$, not both zero. We define their *greatest common divisor* $\gcd(f(x), g(x))$ or $\gcd(f, g)$ as their monic common divisor of greatest degree. (It must exist since $1_{\mathbb{F}}$, of degree 0, is always a monic common divisor. It is unique due to reasons from Unit 4.)

Let $\mathbb{F}$ be a field, and let $a_1(x), a_2(x) \in \mathbb{F}[x]$ with $a_2(x) \neq 0$. We define the $\mathbb{F}[x]$ *Euclidean algorithm* as $(a_1, a_2) \to DA \to (q_1, a_3)$, then $(a_2, a_3) \to DA \to (q_2, a_4)$, and so on until $(a_k, a_{k+1}) \to DA \to (q_k, 0)$.

Bézout's $\mathbb{F}[x]$ Lemma: Let $\mathbb{F}$ be a field, and let $f(x), g(x) \in \mathbb{F}[x]$, not both zero. Then there exist $u(x), v(x) \in \mathbb{F}[x]$ with $f(x)u(x) + g(x)v(x) = \gcd(f(x), g(x))$. Conversely, for any $a(x), b(x) \in \mathbb{F}[x]$, we must have $\gcd(f(x), g(x)) \big| \big(f(x)a(x) + g(x)b(x)\big)$.

$\mathbb{F}[x]$ cancellative property: Let $f, g, h \in \mathbb{F}[x]$, where $\mathbb{F}$ is a field and $f \neq 0$. If $fg = fh$ then $g = h$.

Let R be a commutative ring with identity, and let $a, b \in R$. We say that a is an *associate* of b if there is some unit $u \in R$ with $a = ub$. If $a \in R$ is not a unit and not 0_R, we call a *irreducible* if all of its divisors are units and associates (otherwise we call a *reducible*). We call nonzero nonunit $a \in R$ *prime* if it satisfies

$$\forall b, c \in R, \text{ if } a|bc \text{ then } \big(a|b \text{ or } a|c\big).$$

For Oct. 9:

1. Use the Euclidean algorithm (for integers) to find $[25]^{-1}$ in $\mathbb{Z}_{41}$.
2. Let $n \in \mathbb{Z}$ with $n \geq 2$. Suppose that n is not prime. Find some (nonzero) $[a] \in \mathbb{Z}_n$ that is a zero divisor (and, therefore, not a unit).
3. Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $[a] \in \mathbb{Z}_n$. Prove that $[a]$ is a unit if and only if $\gcd(a, n) = 1$.
4. Prove the $\mathbb{Z}_p$ theorem.

For Oct. 14:

5. Let $\mathbb{F}$ be a field, and let $f(x), g(x) \in \mathbb{F}[x]$ with $f(x), g(x) \neq 0$. Suppose that $(f,g) \to DA \to (q,r)$. Prove that $\gcd(f,g) = \gcd(g,r)$.

6. Prove the $\mathbb{F}[x]$ Euclidean algorithm must terminate at some $(a_k, a_{k+1}) \to DA \to (q_k, 0)$. Prove that when it does that there is some $u \in \mathbb{F}$ with $ua_{k+1} = \gcd(a_1, a_2)$. Use this to find $\gcd(x^3 - x^2 - 4x - 6, x^4 - 2x^3 - 5x^2 + 8x - 6)$ in $\mathbb{Q}[x]$ by hand.

7. If we remember the steps of the $\mathbb{F}[x]$ Euclidean algorithm, we can reverse them, back-substituting repeatedly, to find $u(x), v(x)$ to satisfy Bézout's $\mathbb{F}[x]$ Lemma. Apply this to $(a,b) = (x^3 - x^2 - 4x - 6, x^4 - 2x^3 - 5x^2 + 8x - 6)$, in $\mathbb{Q}[x]$.

8. Prove the uniqueness part of the $\mathbb{F}[x]$ Division Algorithm Theorem. That is, suppose $(f,g) \to DA \to (q,r)$ and also $(f,g) \to DA \to (q',r')$. Prove $q(x) = q'(x)$ and $r(x) = r'(x)$.
   HINT: Write $f = qg + r$ and $f = q'g + r'$. Subtract and rearrange to get $(r - r') = g(q' - q)$. Now think about cases and the degree sum theorem.

For Oct. 16:

9. Let R be a commutative ring with identity, and $a, b, c \in R$. Suppose that a is an associate of b. Prove that b is an associate of a; also, prove that if $a|c$ then $b|c$.

10. Let R be a commutative ring with identity, let $a, b \in R$ with a an associate of b. Prove that if a is irreducible then b is irreducible; also, prove that if a is prime then b is prime.

11. Let $R = \mathbb{F}[x]$, and $a, b \in R$. Prove that the following are equivalent: (i) a, b are associates; (ii) $a|b$ and $b|a$.

12. Let $\mathbb{F}$ be a field. Prove that in $\mathbb{F}[x]$, every irreducible is prime.
    HINT: If $f(x)$ is irreducible and $f(x)|u(x)v(x)$, consider $g(x) = \gcd(f(x), u(x))$. Two cases, one of which is like the proof of Unit 1 Exercise 17 (Bezout).

Extra:

13. Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $[a], [b] \in \mathbb{Z}_n$, with $[a] \neq [0]$. Prove that if $[a]x = [b]$ has no solutions, then $[a]$ is a zero divisor.

14. Let R be a commutative ring with identity. Let $a \in R$ satisfy $a^3 = 0_R$. Prove that $1_R + ax$ is a unit in $R[x]$.

15. Demonstrate, with an example, that the Division Algorithm Theorem need not hold for $\mathbb{Z}[x]$.

16. Let $\mathbb{F}$ be a field, and let $a, b \in \mathbb{F}$ with $a \neq b$. Prove that $\gcd(x + a, x + b) = 1_{\mathbb{F}}$, in $\mathbb{F}[x]$.

17. Let $\mathbb{F}$ be a field, and let $f(x) \in \mathbb{F}[x]$ with $f(x) \neq 0_{\mathbb{F}}$. Suppose that $f(x)|g(x)$ for every nonconstant $g(x) \in \mathbb{F}[x]$. Prove that $deg(f(x)) = 0$.

18. Prove the existence part of the $\mathbb{F}[x]$ Division Algorithm Theorem. That is, prove that for any $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$, there must exist some $q(x), r(x) \in \mathbb{F}[x]$ with $(f,g) \to DA \to (q,r)$.