ETH zürich

Discrete Mathematics **2024**

Student: Jeferson Morales Mariciano <jmorale@ethz.ch>

Assignment 10

Due date: Thursday, 28 November 2024, 23:59

Exercise 10.5, Extension Fields ($\star$) (8 Points)

Let $F = \mathbb{Z}_3[x]_{x^3+2x^2+1}$.

a) Prove that F is a field.

b) Find a generator of F^*. **Show your work**.

c) Find all roots of $a(y) = y^2 + 2y(x^2 + x) + (x^2 + 2)$ in $F[y]$. **Show your work**.

a)

By Definition 5.26, for F to be a field it must be a non-trivial commutative ring F in which every nonzero element is a unit, i.e. $F^* = F \setminus \{0\}$.

Properties of $\mathbb{Z}_3$

Let's check if $\mathbb{Z}_3$ is a field. The short answer positive, given the Theorem 3.23 stating $\mathbb{Z}_p$ is a field if and only if p is prime, which 3 clearly is. This follows from the fact that $\mathbb{Z}_3^* = \mathbb{Z}_3 \setminus \{0\}$ is a multiplicative group. By Theorem 5.13, 5.15 we know that $\langle \mathbb{Z}_3^*; \odot, ^{-1}, 1 \rangle$ is a group, that is is closed under $\odot$, that inherits the associativity of multiplication from the analogous group defined in $\mathbb{Z}_3$, that has a neutral and inverse elements, and that it is cyclic. Moreover, its cardinality is $|\mathbb{Z}_3^*| = \varphi(3) = 2$.

As stated in Example 5.34, using the before-mentioned group we build the ring $\langle \mathbb{Z}_3; \oplus, \ominus, 0, \odot, 1 \rangle$, where we can check that for such algebra: $\langle \mathbb{Z}_3; \oplus, \ominus, 0 \rangle$ is an abelian group, $\langle \mathbb{Z}_3; \odot, 1 \rangle$ is a monoid, and that the distributive and commutative law is inherited from the integers, with its characteristic equal to 3 (Definition 5.19, Example 5.35) and its set of units equal to $\mathbb{Z}_3^*$ (Example 5.39).

As proved at the start, $\mathbb{Z}_3^*$ is a multiplicative group from the fact that for a ring R, R^* is a multiplicative group since it's the group of units of R, by Lemma 5.18. Note that it's also an integral domain since every element is a unit besides 0 and in a commutative ring any unit is not a zerodivisor, as state in Theorem 5.24, concluding that a field is an integral domain.

To conclude, we have shown that the algebra $\langle \mathbb{Z}_3^*; \odot, ^{-1}, 1 \rangle$ is an abelian group, hence $F = \mathbb{Z}_3$ is a field. The field with p elements could be denoted as a Galois Field GF(3).

Properties of $\mathbb{Z}_3[x]$

From Definition 5.25, $\mathbb{Z}_3[x]$ denotes the set of polynomials $a(x)$ in the indeterminate x over the commutative ring and field $\mathbb{Z}_3$, where $a(x) = \sum_{i=0}^{d} a_i x_i$. The degree of $a(x)$ is denoted as $\deg(a(x))$, which is the greatest i for which $a_i \neq 0$.

Recall that for any commutative ring R, $R[x]$ is a commutative ring (Theorem 5.21), that if D is an integral domain, then so is $D[x]$, and that the units of $D[x]$ are the constants polynomials that are units of D, i.e. $D[x]^* = D^*$ (Lemma 5.22). So all this properties get into $\mathbb{Z}_3[x]$, denoting the set of polynomials over the field $\mathbb{Z}_3$.

Properties of $\mathbb{Z}_3[x]_{x^3+2x^2+1}$

Let $m(x)$ be a polynomial of degree d over F, then $F[x]_{m(x)} \stackrel{\text{def}}{=} \{a(x) \in F[x] \mid \deg(a(x)) < d\}$ (Definition 5.34). So $\mathbb{Z}_3[x]_{x^3+2x^2+1}$ is the set of all polynomials over the field $\mathbb{Z}_3$ with degree less than 3. Let F be a finite field with q elements and let $m(x)$ be a polynomial of degree d over F. Then, $|F[x]_{m(x)}| = q^d$ (Lemma 5.34). Hence, the number of polynomial elements in $\mathbb{Z}_3[x]_{x^3+2x^2+1}$ is $|\mathbb{Z}_3[x]_{x^3+2x^2+1}| = |\mathbb{Z}_3|^{\deg(x^3+2x^2+1)} = 3^3 = 27$.

$F[x]_{m(x)}$ is a ring with respect to (w.r.t.) addition and multiplication modulo $m(x)$. (Lemma 5.35). Hence, our last step would be to prove that the ring $\mathbb{Z}_3[x]_{x^3+2x^2+1}$ is a finite extension field of $\mathbb{Z}_3$ with 27 elements. To do so, the ring $F[x]_{m(x)}$ is a field if and only if $m(x)$ is irreducible (Theorem 5.37). I.e. $\forall a(x) \in F$, $\gcd(a(x), m(x)) = 1$ with $a(x) \neq 0 \ \wedge \ \deg(a(x)) < deg(m(x))$, impliying that $a(x)$ is invertible in $F[x]_{m(x)}$.

Let's check if $m(x) = x^3 + 2x^2 + 1$ is irreducible w.r.t. $\mathbb{Z}_3[x]$:

$$\begin{aligned} m(0) = 0^3 + 2 \cdot 0^2 + 1 &= 0 + 0 + 1 = 1 &\equiv_3 1 \\ m(1) = 1^3 + 2 \cdot 1^2 + 1 &= 1 + 2 + 1 = 4 &\equiv_3 1 \\ m(2) = 2^3 + 2 \cdot 2^2 + 1 &= 8 + 8 + 1 = 17 &\equiv_3 2 \end{aligned}$$

Recalling that a root of $a(x) \in R[x]$ is any element $\alpha \in R$ for which $a(\alpha) = 0$ (Definition 5.33), and that for a field F, $\alpha \in F$ is a root of $a(x)$ if and only if $x - \alpha$ divides $a(x)$ (Lemma 5.29), we want to find a root of $m(x) = x^3 + 2x^2 + 1$ in $\mathbb{Z}_3[x]$ with elements $\alpha \in \mathbb{Z}_3$. But as we already tried, there are none. Finally, $\mathbb{Z}_3[x]_{x^3+2x^2+1}$ is a field.

b)

We know from *a)* that the field $\mathbb{Z}_3[x]_{x^3+2x^2+1}$ has cardinality 27. The set of units of the field is $\mathbb{Z}_3^*[x]_{x^3+2x^2+1} = \mathbb{Z}_3[x]_{x^3+2x^2+1} \setminus \{0\}$ with cardinality 26. Proven also by the fact that the multiplicative group of every finite field $\mathrm{GF}(q)$ is cyclic and has order $q-1$ and $\varphi(q-1)$ generators (Theorem 5.40). The factorization of $26 = 2 \cdot 13$, and it follows that we have $\varphi(26) = 12$ generators.

The order of the elements can be either of its divisors, namely $1, 2, 13, 26$ (Corollary 5.10). We need to find an element with order 26, meaning that generates all the units of the field, hence the requested generator.

$$\begin{aligned} x^1 = x &\neq 1 \\ x^2 = x^2 &\neq 1 \\ x^{13} = x^3 + 2x = 2 &\neq 1 \end{aligned}$$

A generator of F is x, since the order of x is not $1, 2, 13$, which left as only option the choice of 26, meaning generating the whole group.

c)

To find all roots of $a(y) = y^2 + 2y(x^2 + x) + (x^2 + 2)$ in $F[y]$ we can precompute, as done in the script, some useful polynomials modulo $m(x)$, i.e. $R_{x^3+2x^2+1}(x^3), R_{x^3+2x^2+1}(x^4)$, where R is the rest.

$$\begin{aligned} &R_{x^3+2x^2+1}(x^3) = -2x^2 - 1 = x^2 + 2 \\ &R_{x^3+2x^2+1}(x^4) = R_{x^3+2x^2+1}(-2x^3 - x) = -2(x^2 + 2) - x = -2x^2 - 4 - x = x^2 + 2x + 2 \end{aligned}$$

Trivially, any constant $0, 1, 2$ of degree zero does not yield a root. We notice that the polynom $a(y)$ has an unusual structure: the term (x^2+2) has no real reason to be in parenthesis but it luckily coincide with $R_{x^3+2x^2+1}(x^3)$. Notice that the field $\mathbb{Z}_3$ once the coefficient of a term a multiple of 3, then it becomes 0 because of modulo 3. The term $3x^3 = 3x^2 + 6$ is achievable by having $2x^3$ from injecting a polynom into $a(y)$ to simplify with the already present term.

Rewrite $a(y) = y^2 + (2x^2 + 2x)y + (x^2 + 2)$. The candidate x seem to be simple good one allowing to simplify:

$$a(x) = x^2 + (2x^2 + 2x) \cdot x + x^3 = x^2 + 2x^3 + 2x^2 + x^3 = 3x^2 + 3x^3 = 0$$

Then, x is a root.
Another way to simplify with x^3 is to increase the degree, i.e. x^2 as polynom, because logically we would still have the same simplification, let's check the candidate x^2:

$$a(x^2) = (x^2)^2 + (2x^2 + 2x) \cdot x^2 + x^3 = x^4 + 2x^4 + 2x^3 + x^3 = 3x^4 + 3x^3 = 0$$

For a field F, a nonzero polynomial $a(x) \in F[x]$ of degree d has at most d roots (Theorem 5.31). There are 2 roots, which are x, x^2, and since $\deg(m(x)) = 2$, there are no more roots to look for.