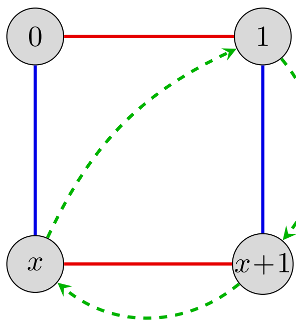
1. The finite field $\mathbb{F}_4$ on 4 elements can be constructed as the quotient of the polynomial $\mathbb{Z}_2[x]$ by the ideal $I = (x^2+x+1)$ generated by the irreducible polynomial x^2+x+1. The figure below shows a Cayley diagram, and multiplication and addition tables for the finite field $\mathbb{Z}_2[x]/(x^2+x+1) \cong \mathbb{F}_4$.



$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

The polynomials $f(x) = x^3+x+1 \in \mathbb{Z}_2[x]$ and $g(x) = x^2+x+2 \in \mathbb{Z}_3[x]$ are irreducible. Construct the Cayley tables and Cayley diagram for the finite fields

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(f) \qquad \text{and} \qquad \mathbb{F}_9 \cong \mathbb{Z}_3[x]/(g)\,.$$

What familiar groups appear as the additive and multiplicative groups of these fields?

2. Let R be a commutative ring with 1.

   (a) Show that R is an integral domain if and only if 0 is a prime ideal.

   (b) Show that an ideal $P \subseteq R$ is prime if and only if R/P is an integral domain.

   (c) Show that every maximal ideal is prime.

   (d) Find the group of units $U(R)$ and the maximal ideal(s) of the ring

   $$R = \Big\{\frac{a}{b} : a, b \in \mathbb{Z},\ \gcd(a,b) = 1,\ p \nmid b\Big\},$$

   where p is a fixed prime number.

3. An ideal $I \subseteq R$ is *radical* if $x^n \in I$ implies that $x \in I$. It is *primary* if $ab \in I$ implies that either $a \in I$ or b^n for some $n \in \mathbb{N}$. An element $r \in R$ is *nilpotent* if r^n for some $n \in \mathbb{N}$.

   (a) Show that $I \subsetneq R$ is radical if and only if R/I has no nonzero nilpotent elements.

   (b) Show that the following are equivalent for $I \subsetneq R$:

      (i) I is prime

      (ii) I is radical and primary

      (iii) The ideal

      $$I[x] := \left\{\sum_{k=0}^{n} a_k x^k \mid a_k \in I\right\}$$

      is a prime ideal of $R[x]$.

(c) Let R be a principal ideal domain. Characterize all nonzero proper ideals that are radical, and all nonzero proper ideals that are primary.

4. Let R be a principal ideal domain. A *common multiple* of $a, b \in R^*$ is an element m such that $a \mid m$ and $b \mid m$. Moreover, m is a *least common multiple* (lcm) if $m \mid n$ for any other common multiple n of a and b.

   (a) Show that any $a, b \in R^*$ have an lcm.

   (b) Show that an lcm of a and b is unique up to multiplication of associates, and can be characterized as a generator of the (principal) ideal $I := (a) \cap (b)$.

5. For any $x = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, define the *norm* of x to be $N(x) = r^2 - ms^2$.

   (a) Show that $N(xy) = N(x)N(y)$.

   (b) Show that $N(x) \in \mathbb{Z}$ if $x \in R_m$.

   (c) Show that $u \in U(R_m)$ if and only if $|N(u)| = 1$.

   (d) Show that $U(R_{-1}) = \{\pm 1, \pm i\}$, $U(R_{-3}) = \{\pm 1, \pm(1 \pm \sqrt{3})/2\}$, and $U(R_m) = \{\pm 1\}$ for all other negative square-free $m \in \mathbb{Z}$.