Problem 1 (Gallian Chapter 13 # 55)**.** Let F be a field of prime characteric p. Prove that

$$K = \{x \in F \mid x^p = x\}$$

is a subfield of F.

Proof. This requires that $1_F \in K$, and that K is closed under addition, additive inverse, multiplication, and multiplicative inverses.

Identity: Since $1^p = x$, $1 \in K$.

Additive inverses: Let $x \in K$. Then $x^p = x$. If $p = 2$, then $-x = x$, so $-x \in K$. Otherwise, p is odd, and $(-x)^p = (-1)^p x^p = (-1)x = -x$, so $-x \in K$.

Multiplicative inverses: Let $x \in K \smallsetminus \{0\}$. Since F is a field, $x^{-1} \in F$. Now $(x^{-1})^p = (x^p)^{-1} = x^{-1}$, so $x^{-1} \in K$.

Multiplication: Let $x, y \in K$. Since x and y commute, $(xy)^n = x^n y^n$ for all $n \in \mathbb{N}$. Thus $(xy)^p = x^p y^p = xy$, so $xy \in K$.

Okay, that was all easy, but addition is a little more subtle.

Addition: Let $x, y \in K$. Recall that the binomial coefficients $\binom{p}{k}$ The Binomial Theorem holds.

By the Binomial Theorem, which holds in an arbitrary commutative ring,

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

Now $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$ is divisible by p unless $k!$ or $(p-k)!$ is divisible by p, so $\binom{p}{k}$ is divisible by p except when $k = 0$ or $k = p$. In F, $p = 0$, so

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

Thus $x + y \in K$. □

Problem 2 (Gallian Chapter 14 # 50)**.** Show that $\mathbb{Z}[i]/\langle 1-i \rangle$ is a field. How many elements does this field contain?

Solution. What is in the ideal $\langle 1-i \rangle$? Well, it is the set of all things divisible by $1-i$. Suppose $1-i \mid a+bi$; then $a+bi = (c+di)(1-i) = (c+d) + i(d-c)$, so $a = c+d$ and $b = d-c$, whence $a+b = 2d$, so $a+b$ is even. On the other hand, if $a+b$ is even, set $c = \dfrac{a-b}{2}$ and $d = \dfrac{a+b}{2}$ to arrive at $a+bi = (c+di)(1-i)$. So $a+bi \in \langle 1-i \rangle$ if and only if $2 \mid a+b$.

Consider the map $\phi : \mathbb{Z}[i] \to \mathbb{F}_2$ given by $a+bi \mapsto a+b \pmod 2$. One easily verifies that this a surjective ring homomorphism. Let $z = a+bi \in \ker(\phi)$ if and only if $a+b \cong 0 \pmod 2$, which occurs if and only if $1-i$ divides z. So $\ker\phi = \langle 1-i \rangle$. By the Isomorphism Theorem, $\mathbb{Z}[i]/\langle 1-i \rangle \cong \mathbb{F}_2$, a field with two elements. □

Problem 3 (Gallian Chapter 14 # 52)**.** How many elements are in the ring $\mathbb{Z}_5[i]/\langle 1+i \rangle$ is a field?

Solution. I believe that $1+i$ is invertible in $\mathbb{Z}_5[i]$, so I attempt to solve $1 = (1+i)(c+di) = (c-d)+(c+d)i$, and get $c-d = 1$ and $c+d = 0$, whence $c = 2^{-1} = 3$ and $d = 2$. That is, $3+2i$ is the inverse of $1+i$, in particular, $1+i$ is invertible, so $\langle 1+i \rangle$ is the whole ring, and $\mathbb{Z}_5[i]/\langle 1+i \rangle$ is the zero ring; it contains 1 element (just zero). □

Problem 4 (Gallian Chapter 15 # 63)**.** Let

$$R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| a, b \in \mathbb{Z} \right\},$$

and let $\phi : R \to \mathbb{Z}$ be given by $\begin{bmatrix} a & b \\ b & a \end{bmatrix} \mapsto a - b$.

(a) Show that ϕ is a homomorphism.

(b) Determine $K = \ker(\phi)$.

(c) Show that R/K is isomorphic to $\mathbb{Z}$.

(d) Is K a prime ideal?

(e) Is K a maximal ideal?

Solution. One computes to verify that ϕ is a homomorphism.

Let $A = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$. Then $A \in K$ if and only if $a - b = 0$, that is, if $a = b$.

Clearly ϕ is surjective, and the image of ϕ is all of $\mathbb{Z}$. By the Isomorphism Theorem, $R/K \cong \mathbb{Z}$.

Since $\mathbb{Z}$ is an integral domain, K is a prime ideal. However, $\mathbb{Z}$ is not a field, so K is not a maximal ideal. □

The following theorem is a consequence of the fact that the multiplicative group of a finite field is cyclic. I'm not sure how to prove it without using, at least indirectly, this fact.

Proposition 1 (Wilson's Theorem)**.** *Let p be a positive prime integer. Then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. This is true if $p = 2$, so assume that p is odd.

In any finite abelian group G, only elements of order two are there own inverses. Thus, if we take the product of all element in G, we obtain the product of the elements of order two, because the other elements cancel each other.

Since $\mathbb{Z}_p$ is a finite field, we know that $G = \mathbb{Z}_p^*$ is cyclic. We know that a cyclic group of order n contains a unique cyclic subgroup of order d for every positive integer d which divides n. Since $|G| = p - 1$ is even, G has a unique element of order two. This element is $\overline{p-1}$. Every other element of G has an inverse which is distinct from it; thus $\prod_{g \in G} g = p - 1$. But $\prod_{g \in G} g = \overline{(p-1)!}$. The result follows. □

Problem 5 (Gallian Chapter 16 # 32)**.** Let $n \in \mathbb{Z}$, $n \geq 2$. Show that $(n-1)! \cong n - 1 \pmod{n}$ if and only if n is prime.

Solution. The reverse direction is Proposition 1.

On the other hand, if n is not prime, $n = pr$ where p is prime and $r > 1$. Then $p \mid (n-1)!$ and $r \mid (n-1)!$, so $n = pr \mid (n-1)!$, which implies that $(n-1)!$ is congruent to zero modulo n. □