Intro to modern algebra II

Instructor: Michael Harris

1. Solution to problem set 5

Problem 1.

Let $k$ be a finite field with $q$ elements. Let $V$ be a $n$–dim $k$–vector space. Let $\{e_{i}|1 \leq i \leq n\}$ be a basis for $V$. Let $v = \sum a_{i}e_{i}$, for $a_{i} \in k$. There are exactly $q$ choices for every coefficient $a_{i}$. Therefore, $|V| = q^{n}$.

Let $k = \mathbb{F}_{3}$ have three elements. Let $f(X) = X^{2} + 1 \in k[X]$. Then $\mathbb{F}_{9} = k[X]/(f)$ is a quadratic extension of $k$ and has nine elements.

Problem 2.

The fact that $R$ is a ring is an exercise in elementary algebra. Let $\sigma(a + b\sqrt{-5}) = a - b\sqrt{-5}$. Let $r = x + y\sqrt{-5}$ and $s = w + z\sqrt{-5}$.

$$\sigma(r)\sigma(s) = (x - y\sqrt{-5})(w - z\sqrt{-5}) = xw - 5yz - (xz + yw)\sqrt{-5} = \sigma(rs)$$

Therefore, $\sigma$ is a homomorphism. For $r \in R$, $N(r) = r\sigma(r) = x^{2} + 5y^{2} \in \mathbb{Z}$.

$$N(rs) = r\sigma(rs) = r\sigma(r)s\sigma(s) = N(r)N(s).$$

Assume that $p = rs$, $p$ a rational prime and $r, s \in R$ as above. Then $N(r)N(s) = N(rs) = N(p) = p^{2}$, thus $N(r)|p^{2}$. If $s \neq \pm 1$ then $N(s) = w^{2} + 5z^{2} > 1$, thus $N(r)|p$.

Assume that $r \notin \mathbb{Z}$. Then $N(r) = x^{2} + 5y^{2} \geq 5y^{2} \geq 5$, as $y \neq 0$.

First we show that 2 and 3 are irreducible:

Assume $3 = rs$ for $r \neq \pm 1$. Then $r, s \notin \mathbb{Z}$. Therefore, $N(rs) = N(r)N(s) \geq 25 > 9 = N(3)$ - a contradiction. The same works for 2.

If $r = 1 + \sqrt{-5}$, $N(r) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 1 + 5 = 6 = 2 \cdot 3$. Thus 6 can be written in two ways as a product of irreducible elements. This is because $R$ is not a UFD. It is a Dedekind domain and with the unique factorization of ideals

$$(6) = (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5})$$

Problem 3. Exercise 50

Let $F$ be a field $p(X) \in F[X]$ and irreducible polynomial. Prove that if $g(X) \in F[X]$ then either $(p(X), g(X)) = 1$ or $p(X)|g(X)$.

Recall that $F[X]$ is an Euclidean domain if $F$ is a field. Thus by the Euclidean algorithm $(p(X), g(X)) = (f(X))$ where $f(X)$ is the greatest common divisor of $p(X)$ and $g(X)$. Since $p(X)$ is irreducible either $f(x)$ is constant or a constant multiple of $p(X)$ (recall that the constant polynomials in $F[X]$ are the units in this ring). The claim follows.

Problem 4. Exercise 53

Part (i): Assume that $(0)$ is a prime ideal. Then if $ab \in (0)$, $a \in (0)$ or $b \in (0)$. Thus there are no zero divisors or equivalently $R$ is an integral domain.

Assume that $R$ is an integral domain and $ab \in (0)$. Since $a, b$ are not zero divisors, $a \in (0)$ or $b \in (0)$. Thus $(0)$ is a prime ideal.

Part (ii): Recall that $a$ is a maximal ideal iff $R/a$ is a field. Since $R \cong R/(0)$, the claim follows.

Problem 5.

Let $I \subset \mathbb{Z}[X]$ be the set of polynomials with even constant term. One can easily check that $I = (X, 2)$ is an ideal and that $1 \notin I$. Then by the third isomorphism theorem $\mathbb{Z}[X]/I = \mathbb{Z}/2\mathbb{Z}$, which is a field. Thus $I$ is maximal.

Problem 6. Exercise 63
Let \((r,s) = 1\) and \(\frac{r}{s} \in \mathbb{Q}\) be a root for \(f(X) = a_nX^n + \ldots + a_0\). Plugging in \(\frac{r}{s}\) and multiplying by \(s^n\) we get

\[
a_n\frac{r^n}{s^n} + a_{n-1}\frac{r^{n-1}s}{s^n} + \ldots + a_0 = 0
\]

Since \(r\) must divide the LHS and it appears in all terms except the last it must divide it too. Since \((r,s) = 1\) it follows that \(r|a_0\). Similarly \(s|a_n\), hence \(s|a_n\).

**Problem 7. Exercise 65**

Let \(f(X) = a_nX^n + \ldots + a_0 \in F[X]\) is an irreducible polynomial. Then so is \(g(X) = a_0X^n + \ldots + a_n\). Assume that \(g(X) = h(X)k(X)\) for

\[
h(X) = \sum_{i=0}^{r} b_iX^i
\]

\[
k(X) = \sum_{i=0}^{s} c_iX^i
\]

Thus

\[
a_0X^n + \ldots + a_n = (b_rX^r + \ldots + b_0)(c_sX^s + \ldots + c_0)
\]

Make the change of variables \(X \mapsto 1/X\) and multiply by \(X^n\) to get that

\[
a_nX^n + \ldots + a_0 = (b_0X^r + \ldots + b_r)(c_0X^s + \ldots + c_s)
\]

Thus \(f(X)\) is also reducible.

**Problem 8. Exercise 66**

Let \(\phi : R[X] \to R[X]\) be defined by \(f(X) \mapsto f(X + c)\) for some \(c \in R\). Then \(\phi\) is an isomorphism of rings, because by definition it is a homomorphism and its inverse is \(\phi^{-1} : f(X) \mapsto f(X - c)\). If \(p(X) = f(X)g(X)\) then \(\phi(p) = \phi(f)\phi(g)\) and thus \(p(X + c)\) is also reducible. The converse holds for \(\phi^{-1}\).