ALGEBRA 2 NOTES FOR THE FEBRUARY 9 LECTURE

MARK H. KIM

1. Eisenstein Irreducibility Criterion

Theorem 1.1 (Eisenstein irreducibility criterion). Let \( f(x) = a_0 + a_1x + \cdots + a_Nx^N \in \mathbb{Z}[x] \). If there exists a prime number \( p \) such that
\[
\begin{align*}
& \bullet \quad p \mid a_0, \ldots, a_{N-1}, \\
& \bullet \quad p \nmid a_N, \text{ and} \\
& \bullet \quad p^2 \nmid a_0,
\end{align*}
\]
then \( f(x) \) is irreducible over \( \mathbb{Q} \). In particular, \( f(x) \) is irreducible over \( \mathbb{Z} \).

Proof. We establish the contrapositive. To this end, we suppose that \( f(x) \) is reducible, so that we can find non-unit polynomials \( g(x) = b_0 + \cdots + b_sx^s \) and \( h(x) = c_0 + \cdots + c_tx^t \) such that \( f(x) = g(x)h(x) \). Let \( \phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x] \) be given by the formula \( \phi(a(x)) = \overline{a(x)} \), where \( \overline{a(x)} \) denotes the polynomial in \( \mathbb{Z}_p[x] \) obtained by replacing the coefficients of \( a(x) \) with the corresponding equivalence classes in \( \mathbb{Z}_p \). Observe that \( \overline{g(x)} \overline{h(x)} = \overline{f(x)} = \overline{a_Nx^n} \), whence \( \overline{g(x)} = \overline{b_sx^s} \) and \( \overline{h(x)} = \overline{c_tx^t} \). It follows that \( p \mid b_0 \) and \( p \mid c_0 \), so that \( p \mid b_0c_0 = a_0 \). \( \square \)

Example 1.2. For \( g(x) = x^3 - 2 \), a simple choice like \( p = 2 \) would do. \( \square \)

Example 1.3. Let \( p \) be an arbitrary prime number and define
\[
\begin{align*}
g(x) = \frac{x^p - 1}{x - 1} &= 1 + x + \cdots + x^{p-1}.
\end{align*}
\]
Then
\[
\begin{align*}
g(x + 1) &= \frac{(x + 1)^p - 1}{(x + 1) - 1} = x^{p-1} \left( \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \binom{p}{p-1} \right).
\end{align*}
\]
Observe that \( p \nmid 1 \) and \( p^2 \nmid 1 \). Moreover, \( p \mid \binom{p}{1}, \ldots, \binom{p}{p-1} \), and so we can invoke the Eisenstein criterion (Theorem 1.1) to conclude that \( g(x + 1) \) is irreducible over \( \mathbb{Q} \). \( \square \)

Let \( F \) be a field. Since \( F[x] \) is a Euclidean domain, \( F[x] \) is a unique factorization domain. This, in particular, implies that every \( g(x) \in F[x] \) can be written in the form
\[
g(x) = \prod_i p_i(x)^{m_i},
\]
where the \( p_i(x) \) are irreducible polynomials in \( F[x] \).

Date: Monday 9th February, 2015, 12:17.
Recall that a principal ideal \((g(x))\) of \(F[x]\) is included in another principal ideal \((h(x))\) in \(F[x]\) if and only if \(h(x) \mid g(x)\). This, in particular, implies that \((g(x)) = (h(x))\) if and only if \(h(x) = cg(x)\) for some nonzero \(c \in F\). Since \(F[x]\) is a principal ideal domain, we see that inclusion relations of ideals of \(F[x]\) can be characterized by factorizability of the polynomials that generate the ideals. We formalize this observation below.

**Definition 1.4.** A maximal ideal of a ring \(R\) is a proper ideal \(I\) of \(R\) such that no proper ideal of \(R\) properly contains \(I\).

**Theorem 1.5.** In a principal ideal domain \(D\), an ideal \((\alpha)\) of \(D\) is maximal if and only if \(\alpha\) is irreducible in \(D\).

**Proof.** If \(\alpha\) is reducible, then we can find non-units \(\beta, \gamma \in D\) such that \(\alpha = \beta \gamma\). This implies that

\[(\alpha) \subset (\beta) \subset D.\]

Now, \((\alpha) \neq (\beta)\), as \(\gamma\) is not a unit. Similarly, \((\beta) \neq D\), as \(\beta\) is not a unit. Therefore, the inclusions relations above are strict, and so \((\alpha)\) fails to be maximal.

Conversely, if \((\alpha)\) is not maximal, then we can find a proper ideal \(J\) of \(D\) that contains \((\alpha)\). Since \(D\) is a PID, we can find \(\beta \in D\) such that \((\beta) = J\). This implies that \(\beta \mid \alpha\), and so there exists a \(\gamma \in D\) such that \(\alpha = \beta \gamma\). \(\beta\) is not a unit, as \((\beta) \neq D\); \(\gamma\) is not a unit, as \((\alpha) \neq (\beta)\). \(\square\)

Let us now consider the ring \(R = K[x]/(f(x))\), where \(K\) is a field and \(f(x)\) is a degree-\(n\) polynomial in \(K[x]\). Elements of \(R\) are of the form

\[a_0 + a_1x + \cdots + a_{n-1}x^{n-1},\]

where \(a_0, \ldots, a_{n-1} \in K\).

Think, for example, \(F = \mathbb{Q}[x]/(x^3 - 2)\). This is a field, in fact. To see this, we fix \(g(x) = a + bx + cx^2 \in F\). Since \(x^3 - 2\) is irreducible over \(\mathbb{Q}\) (see Example 1.2), we see that \(\gcd(g(x), x^3 - 2) = 1\). It then follows from Bezout’s lemma that there exist \(r(x), s(x) \in \mathbb{Q}[x]\) such that

\[g(x)r(x) + (x^3 - 2)s(x) = 1.\]

Therefore, in \(\mathbb{Q}[x]/(x^3 - 2)\), we obtain the relation

\[1 = \overline{g(x)} \overline{r(x)} + \overline{(x^3 - 2)s(x)} = \overline{g(x)} \overline{r(x)} + 0 \overline{s(x)} = \overline{g(x)} \overline{r(x)},\]

whence \(\overline{g(x)}\) is invertible in \(\mathbb{Q}[x]/(x^3 - 2)\). Since the choice of \(g(x)\) was arbitrary, we conclude that \(F\) is a field.

We generalize our observation as follows:

**Theorem 1.6.** Let \(K\) be a field and let \(R = K[x]/(f(x))\). If \(f(x)\) is irreducible in \(K[x]\), then \(R\) is a field.

**Proof.** Postponed to a later class. \(\square\)

2. **Vector Spaces**

**Definition 2.1.** \(V\) is a vector space over a field \(F\) if there exist the addition operation \(+ : V \times V \to F\) and scalar multiplication operation \(\cdot : F \times V \to V\) such that

1. \((V, +)\) is an abelian group:
(2) the distributive property holds, viz., for all \( v, w \in V \) and \( \alpha, \beta \in F \),
\[
\alpha(v + w) = \alpha v + \alpha w \quad \text{and} \quad (\alpha + \beta)v = \alpha v + \beta v;
\]
(3) if \( \alpha, \beta \in F \) and \( v \in V \), then \( \alpha(\beta v) = (\alpha \beta)v \);
(4) \( 1_F v = v \) for all \( v \in V \).

**Example 2.2.** For each field \( F \), the set of \( N \)-tuples
\[
F^N = \{(a_1, \ldots, a_N) : a_i \in F\}
\]
is a vector space over \( F \) with respect to coordinatewise addition
\[
(a_1, \ldots, a_N) + (b_1, \ldots, b_N) = (a_1 + b_1, \ldots, a_N + b_N)
\]
and coordinatewise scalar multiplication
\[
\alpha(a_1, \ldots, a_N) = (\alpha a_1, \ldots, \alpha a_N).
\]

**Example 2.3.** For each field \( F \), the ring of polynomials \( F[x] \) is a vector space over \( F \) with respect to ring addition in \( F[x] \) and ring multiplication restricted to \( F \times F[x] \). Note also that, for each \( N \in \mathbb{N} \), the set
\[
\{a_0 + \cdots + a_{N-1}x^{N-1} : a_0, \ldots, a_{N-1} \in F\}
\]
constitutes a vector space over \( F \) as well. (This is called a linear subspace of \( F[x] \).)

**Example 2.4.** The set of all sequences in a field \( F \) is a vector space over \( F \) with respect to termwise addition and termwise scalar multiplication.

**Example 2.5.** If \( K \) is a field and if \( F \) is a subfield of \( K \), then \( K \) is a vector space over \( F \) with respect to field addition in \( K \) and field multiplication in \( K \) restricted to \( F \times K \). In particular, every field is a vector space over itself.