

**Frank Moore**  
**Algebra 901 Notes**  
**Professor: Tom Marley**

Let  $R$  be a commutative ring with  $1_R$ . Since  $(R, +)$  is an abelian group, we can let  $\mathbb{Z}$  act on  $R$  as follows: for  $m \in \mathbb{Z}$ ,  $r \in R$ , define

$$mr = \begin{cases} \sum_{i=1}^m r & m > 0 \\ \sum_{i=1}^m (-r) & m < 0 \\ 0 & m = 0 \end{cases}$$

Note that the above turns  $(R, +)$  into a  $\mathbb{Z}$  module, and that the above definition in fact works for any abelian group. Let  $P = \langle 1_R \rangle = \{m \cdot 1_R \mid m \in \mathbb{Z}\}$  where  $\langle 1_R \rangle$  is the  $\mathbb{Z}$ -submodule generated by  $1_R$  in  $(R, +)$ . Of course,  $P$  is a cyclic group under  $+$  but it is in fact a subring of  $R$  since  $(m \cdot 1_R)(n \cdot 1_R) = (mn) \cdot 1_R \in P$ .

**Definition:**  $P = \langle 1_R \rangle$  is called the **prime subring** of  $R$  and  $P$  is clearly the smallest subring of  $R$  containing  $1_R$ . For some examples, the prime subring of  $\mathbb{Q}$  is  $\mathbb{Z}$  and the prime subring of  $\mathbb{Z}_n$  is  $\mathbb{Z}_n$ .

Now, consider the ring map  $\phi : \mathbb{Z} \rightarrow R$  sending  $m \mapsto m \cdot 1_R$ . By definition,  $P = \mathfrak{I}(\phi)$ , and we also have that  $\ker(\phi) = (n)$  where  $n \geq 0$ .

**Definition:** If  $\ker \phi = (n)$ ,  $n \geq 0$ , then  $R$  is said to have **characteristic  $n$** . Since  $P \cong \mathbb{Z}/\ker \phi = \mathbb{Z}/(n)$ , we have that if  $R$  has characteristic  $n$  then  $P \cong \mathbb{Z}_n$  and if  $R$  has characteristic zero, then  $P \cong \mathbb{Z}$ .

**Examples:** The characteristic of  $\mathbb{Q}, \mathbb{Z}, \mathbb{R}$ , or  $\mathbb{C}$  are all zero.  $\text{Char } \mathbb{Z}_n[x]/(x^2 - 3) = n$ .  $\text{Char } \mathbb{Z}_6 \times \mathbb{Z}_8 = 24 = \text{lcd}(6, 8)$ . As a remark, if  $R$  is a domain, then the characteristic of  $R = 0$  or  $p$ ,  $p$  a prime (else we would have zerodivisors in  $R$ ).

**Definition:** If  $F$  is a field, then the prime subfield of  $F$  is the smallest subfield of  $F$  containing  $1_F$ . Certainly the prime subfield contains the prime subring. Also the characteristic of  $F = 0$  or  $p$ ,  $p$  a prime. If the characteristic of the field is  $p$ , then  $P = \mathbb{Z}_p$  and  $P$  is already a field, so the prime subring equals the prime subfield. If  $\text{Char } F = 0$ , then  $P \cong \mathbb{Z}$  and so the prime subfield has to be  $\mathbb{Q}$ .

**Definition:** Let  $f(x) \in F[x]$  be a polynomial and  $\alpha \in \bar{F}$  be a root of  $f(x)$ . Then  $\alpha$  is called a multiple root of  $f(x)$  if  $(x - \alpha) \mid f(x)$  in  $\bar{F}[x]$ .

**Definition:** Let  $f(x) \in F[x]$ ,  $f(x) = c_n x^n + \dots + c_1 x + c_0$ . Define the derivative of  $f(x)$  by

$$f'(x) = (nc_n)x^{n-1} + ((n-1)c_{n-1})x^{n-2} + \dots + c_1 \in F[x]$$

Check that the normal rules for derivative like linearity, product rule and chain rule still work (they do).

**Proposition:** Let  $f(x) \in F[x]$  and  $\alpha \in \bar{F}$  be a root of  $f(x)$ . Then  $\alpha$  is a multiple root of  $f(x) \Leftrightarrow f'(\alpha) = 0$ .

*Proof:* If  $\alpha$  is a multiple root, then  $f(x) = (x - \alpha)^2 g(x)$ . Then  $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$ , so that  $f'(\alpha) = 0$ . Conversely, suppose that  $f'(\alpha) = 0$  and write  $f(x) = (x - \alpha)h(x)$ . Then  $f'(x) = h(x) + (x - \alpha)h'(x)$ , hence  $0 = f'(\alpha) = h(\alpha)$ . By the root theorem,  $(x - \alpha)$  is a factor of  $h(x)$ , so write  $h(x) = (x - \alpha)g(x)$ , hence  $f(x) = (x - \alpha)^2 g(x)$  as desired.

**Theorem:** Let  $f(x) \in F[x] \setminus F$ . Then  $f(x)$  has multiple roots  $\Leftrightarrow \gcd(f, f') = 1$ .

*Proof:* If  $f(x)$  has no multiple roots then  $f$  and  $f'$  have no common root in  $F$ . Therefore,  $\gcd_{\bar{F}}(f, f') = 1 = \gcd_F(f, f')$ . For the reverse direction, if  $\gcd_F(f, f') = 1$  then  $f$  and  $f'$  have no common factors in  $\bar{F}$ . Therefore  $f$  and  $f'$  have no common roots, hence  $f$  has no multiple roots.

**Theorem:** Let  $f(x)$  be an irreducible polynomial in  $F[x]$ .

1. If  $\text{Char } F = 0$  then  $f(x)$  has no multiple roots.
2. If  $\text{Char } F = p$  then  $f(x)$  has multiple roots  $\Leftrightarrow f(x) = g(x^p)$  for some  $g(x) \in F[x]$ , i.e.  $f(x) = a_n x^{pn} + a_{n-1} x^{p(n-1)} + \cdots + a_1 x^p + a_0$ .

*Proof:* Certainly,  $\deg f'(x) < \deg f$ . Since  $f(x)$  is irreducible,  $\gcd(f', f) = 1$  or  $cf$  for some  $c \in F$ . If  $f'(x) \neq 0$ , then  $cf \nmid f'$  so  $\gcd(f, f') = 1$ . Therefore,  $\gcd(f, f') \neq 1 \Leftrightarrow f'(x) = 0$ . So, in case 1) this cannot happen since we are in characteristic zero. If the  $\text{Char } F = p$ , then  $f'(x) = 0 \Leftrightarrow$  the only nonzero coefficients occur in front of powers of  $x$  to a multiple of  $p$ , i.e.  $f(x) = g(x^p)$  for some  $g \in F[x]$ .

Note that if  $|F| < \infty$  then  $\text{Char } F = p$  where  $p$  is a prime. In fact,  $\mathbb{Z}_p \subseteq F$ .

**Proposition:** If  $|F| < \infty$  then  $|F| = p^n$  where  $p = \text{Char } F$ .

*Proof:*  $F \supseteq \mathbb{Z}_p$  and as  $|F| < \infty$ ,  $F/\mathbb{Z}_p$  is algebraic, with  $[F : \mathbb{Z}_p] = n$ . So, as a  $\mathbb{Z}_p$  vector space,  $F \cong (\mathbb{Z}_p)^n$  and hence  $|F| = p^n$ .

**Remark:** If  $\text{Char } R = p$ , where  $p$  is a prime, then  $(a + b)^p = a^p + b^p$  by the binomial theorem. In fact, we get that  $(a + b)^{p^n} = a^{p^n} + b^{p^n}$  for any  $n \geq 1$ . The function

$$\begin{aligned} \phi : R &\rightarrow R \\ a &\mapsto a^p \end{aligned}$$

is a ring homomorphism for this reason and is called the **Frobenius endomorphism**.

**Theorem:** Let  $p$  be a prime and  $n \geq 1$ . Then there exists a field of order  $p^n$ . Moreover, any field of order  $p^n$  is a splitting field of  $x^{p^n} - x$  over  $\mathbb{Z}_p$ . Hence, any two finite fields of the same order are isomorphic.

*Proof:* Let  $p, n$  be given. Let  $F$  be a splitting field for  $f(x) = x^{p^n} - x$  over  $\mathbb{Z}_p$ . Let  $S = \{\alpha \in F \mid f(\alpha) = 0\}$ . Since  $f'(x) = -1$ ,  $f(x)$  has  $p^n$  distinct roots in  $F$ , and hence  $|S| = p^n$ . We claim that  $S = F$ . It is enough to show that  $S$  is a field, since  $F$  was the splitting field for  $x^{p^n} - x$  and certainly has to contain all its roots. By a HW exercise (If  $E/F$  is an algebraic field extension and  $R$  a subring of  $E$  that contains  $F$ , then  $R$  is a field), it is enough to show that  $S$  is a ring, so it is enough to check that  $S$  is closed under  $+$  and  $*$ .  $*$  is easily checked, and for  $+$ , note that if  $\alpha, \beta \in S$ , we have that  $(\alpha + \beta)^{p^n} - (\alpha + \beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0$ , so  $\alpha + \beta \in S$ . Therefore  $S = F$  and  $|F| = p^n$ .

Now let  $E$  be a field of order  $p^n$ ,  $p$  a prime. So  $\text{Char } E = \text{Char } F = p$ . Therefore  $\mathbb{Z}_p \subseteq E$ . Note that  $|E^\times| = p^n - 1$ , where  $E^\times$  denotes the group of units of  $E$ . By Lagrange's Theorem, we have that  $\alpha^{p^n-1} = 1$  for all  $\alpha \in E^\times$ , and this  $\alpha^{p^n} = \alpha$  for all  $\alpha \in E$ . So, every element in  $E$  is a root of  $x^{p^n} - x \in \mathbb{Z}_p[x]$ . Certainly  $E$  is a splitting field of  $x^{p^n} - x$ , and hence  $E \cong F$ .

**Proposition:** Let  $F$  be a field of order  $p^n$ . Then  $F$  is the splitting field of an irreducible polynomial in  $\mathbb{Z}_p[x]$  of deg  $n$ .

*Proof:* As  $F$  is a finite field,  $F^\times$  is cyclic. Let  $F^\times = \langle \alpha \rangle$ . Certainly,  $F = \mathbb{Z}_p(\alpha)$ . Since  $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n$ , we have that  $f(x) = \text{Irr}(\alpha, \mathbb{Z}_p)$  has degree  $n$ . Now, note that  $F/\mathbb{Z}_p$  is normal since it is the splitting field of  $x^{p^n} - x$ . Hence  $f(x)$  splits in  $F$  since it has a root in  $F$ . Therefore  $F$  is the splitting field for  $f(x)$ .