Abstract Algebra

August, Evelyn

12/09/2021

$\boxed{\text{7: proposition}}$ Let R be a finite commutative ring with unity. Then for all $r \neq 0 \in R$, r is a unit or a zero divisor.

$\boxed{\text{proof}}$ Suppose r is not a zero divisor. Since R is finite, it follows that the sequence ${r^n}_{n\in\mathbb{Z}}$ must be finite as well by closure. Hence $r^i = r^j$ for some integers i, j such that $i \neq j$. Without loss of generality assume $i > j$. We know that $r^i \neq 0$ and $r^j \neq 0$, because if they were, by the supposition that r is a not a zero divisor $rr^{i-1} = 0$ hence r^{i-2} all the way to $r = 0$, contradicting the supposition that r is nonzero. By properties of additive inverses in a Ring, we know that r^j exists. Consider $r^i - r^j = 0$. By properties of distribution it follows that $r^i - r^j = r^j(r^{i-j} - 1) = 0$. Since r is not a zero-divisor, we know that either r^i or $(r^{j-i} - 1)$ is equal to zero. We explained earlier that $r^i \neq 0$. Thus, $(r^{j-i} - 1)$ must equal zero, which implies that $r^{j-i} = 1$ or in other words $rr^{j-i-1} = 1$, saying that r^{j-i-1} is the inverse of r. Hence, r is a unit. QED.

$\boxed{\text{35: proposition}}$ Let F be a field of order 2^n. Prove that $charF = 2$.

$\boxed{\text{proof}}$ Let F be a field with order 2^n. Since F is a field, it is also an integral domain, an by Theorem 13.4 it follows that $charF$ is 0 or p for some prime p. Since fields are also rings with unity 1, it follows by Theorem 13.3 that the order of 1 is equal to $charF$, so the order of 1 is either 0 or prime. By corollary 2 of Lagrange's Theorem, it follows that the order of each element in F divides the order of F, since $|F|$ is finite. Thus, the order of 1 needs to divide 2^n, so it cannot be 0, leaving us with the prime option. By the Fundamental Theorem of Arithmetic, up to rearrangement of the factors, the prime factorization of a natural number greater than 1 is unique. Hence, the only prime that divides 2^n is 2, so the order of 1 is 2 and thus $charF = 2$. QED.

$\boxed{\text{lemma}}$ given a prime number p, each pth

$\boxed{\text{lemma}}$ (The generalized N∅∅B binomial theorem)

$\boxed{\text{proof}}$

$\boxed{\text{63: proposition}}$ Let F be a field with char$F = p$ for some prime p. Prove that $K = \{x \in F | x^p = x\}$ is a subfield in F.

$\boxed{\text{proof}}$ Notice that by definition of unity and the additive identity, $0^p = 0$ and $1^p = 1$, hence $0, 1 \in K$ and there are at least two elements in K. We proceed then by the finite subfield test. Let F and K be defined as above. This proof is going to apply the subfield test, so we want to show that $a - b \in K$ and $ab^{-1} \in K$ for some $a, b \in K$.
Let a, b be arbitrary elements in K. Consider $a - b = a + (-b) = a + (-1)b$. Since $a, b \in K$, it follows by definition of K that $a - b = a^p + (-1)b^p$. Because p is odd by restriction of it being prime other than 2 (if it's 2 then...), $(-1)^p = (-1)$, hence $a - b = a^p + (-1b)^p = a^p + (-b)^p$. By problem 49$a$ in this chapter it follows that $a^p + (-b)^p = (a + (-b))^p = (a - b)^p$ and hence by definition of K we know that $a - b = (a - b)^p \in K$. If $\Gamma F = 2$, then $(a - b)^2 = (a - b)(a - b) = a^2 - 2 \cdot ab + (-b)(-b) = a^2 + b^2$. But since char$F$=2, we know that $2a = a + a = 0$, which means that $a = -a$ for all $a \in F$. It follows that $a^2 + b^2 = a^2 - b^2$.

Furthermore, consider ab^{-1}. We want to show that $(ab^{-1})^p = ab^{-1}$, as this would imply that $ab^{-1} \in K$. By the associative and commutative property of multiplication in a field, $(ab^{-1})^p = a^p(b^{-1})^p = a(b^{-1})^p$, as follows from the definition of K and the fact that $a \in K$. It remains to be shown that $(b^{-1})^p = b^{-1}$. Clearly $(b^{-1})^p \in F$ by definition of a field and closure. Consider $(b^{-1})^p b$. Since by the associative and commutative properties of multiplication in a field, and by definition of the multiplicative inverse $b^p = b$, $(b^{-1})^p b = (b^{-1})^p b^p = (b^{-1})^p b^p = (b^{-1}b)^p = 1^p = 1$, where 1 is unity in F. Hence by definition of the multiplicative inverse, $(b^{-1})^p = b^{-1}$, so by substitution $(ab^{-1})^p = ab^{-1}$, hence by definition of K $ab^{-1} \in K$.

Since a and b are arbitrary elements of K, it follows that for all $a, b \in K$, $a - b \in K$ and $ab^{-1} \in K$. So by the subfield field test it follows that K is a subfield of F. QED.

$\boxed{\text{3: proposition}}$ Verify that $I =< a_1, ...a_n >= \{r_1a_1 + ... + r_na_n | r_i \in R\}$ for $a_1, ...a_n \in R$ and R is a commutative ring with unity.

$\boxed{\text{proof}}$ Let x, y be arbitrary elements in I. Then $x = r_1a_1 + ... + r_na_n$ and $y = r'_1a_1 + ... + r'_na_n$ for $a_i, r_i, r'_i \in R$. Clearly, I is non-empty. Consider $x - y = r_1a_1 + ... + r_na_n - (r'_1a_1 + ... + r'_na_n) = r_1a_1 + ... + r_na_n - r'_1a_1 - ... - r'_na_n = r_1a_1 - r'_1a_1 + ... + r_na_n - r'_na_n = (r_1 - r'_1)a_1 + ... + (r_n - r'_n)a_n$ (By the properties of a ring and theorem 12.1). But since R is closed by properties of a ring, $r_i - r'_i \in R$ and thus $x - y \in I$.
Next, consider rx for $r \in R, x \in I$. Then $rx = r(r_1a_1 + ... + r_na_n) = rr_1a_1 + ... + rr_na_n = (rr_1)a_1 + ... + (rr_n)a_n$ by the distributive property and associative property of multiplication in a ring. But since R is closed under multiplication, $rr_i \in R$ and $rx = rr_1a_1 + ... + rr_na_n \in I$. Likewise for xr, as the commutativity of R implies that $xr = rx$. Since x and y were arbitrary, it follows for all $x, y \in I$ and for all $r \in R$, $x - y \in I$ and $ar = ra \in R$. Hence by the Ideal Test it follows that I is an ideal of R. QED.

$\boxed{\text{3: proposition II}}$ If J is any ideal of R that contains $a_1, ...a_n$, then $I \subseteq J$.

$\boxed{\text{proof}}$ Let I and J be defined as above. Let x be an arbitrary element in I. Then $x = r_1a_1 + ... + r_na_n$ for $r_i, a_i \in R$, as follows by definition of I. Furthermore, since $r_1, \ldots, r_n \in R$, it follows by definition of an ideal that, as J is an ideal of R, $r_1a_1, \ldots, r_na_n \in J$. Furthermore, since ideals are subrings, which are closed under the additive operation, it follows that $r_1a_1 + r_2a_2 \in J$. Hence by associativity $(r_1a_1 + r_2a_2) + r_3a_3 = r_1a_1 + r_2a_2 + r_3a_3 \in J$. Continuing on until each multiple is added in, we arrive at $x = r_1a_1 + \ldots r_na_n \in J$. Since x is an arbitrary element of I, it follows that for all $x \in I$, $x \in J$ as well. Hence by definition of a subset, $I \subseteq J$.
Q.E.D.

$\boxed{\text{proposition : 29}}$ In $\mathbb{Z}[x]$, let $I = \{f(x) \in \mathbb{Z}[x] : f(0) = 0\}$. Then $I =< x >$.

$\boxed{\text{proof}}$ First, we digest what this statement means. Note that $< x >= \{g(x)x : g(x) \in \mathbb{Z}[x]\}$. Both I and $< x >$ are sets, hence this will be a set equality proof, as the operations are directly inherited from the ring which these two things are ideals of.
To prove that $< x > \subseteq I$, take some arbitrary $f(x) \in < x >$. By definition of $< x >$, $f(x) = g(x)x$ for some $g(x) \in \mathbb{Z}[x]$. By definition of $\mathbb{Z}[x]$, $g(x) = a_1 + a_2x + \ldots a_nx^{n-1}$ for some $a_1, \ldots a_n \in \mathbb{Z}$ and non-negative integer $n - 1$. Substituting back in and applying the distributive and associative laws, and using the fact that polynomial multiplication is commutative, we find $f(x) = g(x)x = (a_1 + a_2x \ldots a_nx^{n-1})x = a_1x + a_2x^2 + \ldots a_nx^n$. Now evaluating $f(0)$, we have, by the properties of a ring, $a_1(0) + \ldots a_n(0)^n = 0$. Hence by definition of I, $f(x) \in I$. Since $f(x)$ is an arbitrary element in $< x >$, it follows that for all $f(x) \in I$, $f(x) \in I$. Hence $< x > \subseteq I$.
To prove that $I \subseteq < x >$, let $f(x) \in I$ be arbitrary. Since $f(x) \in \mathbb{Z}[x]$ by definition of I, $f(x) = a_0 + a_1x + \ldots a_nx^n$ for some $a_1, \ldots, a_n \in \mathbb{Z}$ and some $n \in \mathbb{N}^0$, and since $f(0) = a_0 + a_1x + \ldots a_nx^n = a_0 + a_10 + \ldots a_n0^n = a_0 + 0 = a_0$, we have that $a_0 = 0$. Hence by

the distributive property of rings $f(x) = a_1 x + \ldots a_n x^n = x(a_1 + \cdots + a_n x^{n-1})$. By definition of $\mathbb{Z}[x]$, $a_1 + \cdots + a_n x^{n-1} \in \mathbb{Z}[x]$, hence by definition of $< x >$, $f(x) \in < x >$. Since $f(x)$ is arbitrary it follows that for all elements $f(x) \in I$, $f(x) \in < x >$ as well. Hence $I \subseteq < x >$.
Since $< x > \subseteq I$ and $I \subseteq < x >$, it follows by definition of set equality that $< x > = I$.
Q.E.D.

$\boxed{\text{problem : 39}}$ Let $I = < x^2 + x + 2 >$ be the principle ideal of $x^2 + x + 2$ in $\mathbb{Z}_5[x]$. Find the multiplicative inverse of $2x + 3 + I$ in the factor ring $\mathbb{Z}_5[x]/I$.

$\boxed{\text{solution}}$ First, note that the multiplicative identity is $1 + I$, not I. This can be seen easily, as $(1 + I)(f(x) + I) = 1f(x) + I = f(x) + I$ for all $f(x) \in \mathbb{Z}_5[x]$. Hence we are looking for an element in the factor ring, $f(x) + I \in \mathbb{Z}_5[x]/I$, represented by some polynomial $f(x) \in \mathbb{Z}_5[x]$, such that $(f(x) + I)(2x + 3 + I) = 1 + I$.

Notice that, should such an element exist, it would follow by definition of the factor ring and by properties of cosets that, $(f(x) + I)(2x + 3 + I) = f(x)(2x + 3) + I = 1 + I$, hence $(f(x))(2x + 3) - 1 \in I$. By definition of I, this means that $(f(x))(2x + 3) - 1 = (x^2 + x + 2)g(x)$ for some $g(x) \in \mathbb{Z}_5[x]$. Luckily, only a couple guesses lead to the observation that $(2x + 3)(3x + 1) = 6x^2 + 11x + 3 = x^2 + x + 3 = (x^2 + x + 2) + 1$. So the multiplicative inverse of $2x + 3 + I$ in $\mathbb{Z}_5[x]/I$ is $3x + 1 + I$.