Basic Algebra 1
Solutions of Assignment 6

Solution of the problem 1. Starting with prime number 3 and looking for a root, we see that $f(x) = x^2 + 1$ has no zero in $\mathbb{Z}_3$, hence it is irreducible in $\mathbb{Z}_3[x]$. Next consider 5. This case is actually different. In fact in $\mathbb{Z}_5[x]$ we have the factorization $f(x) = (x + 2)(x + 3)$. Continuing this way, we find that $f(x)$ is irreducible in $\mathbb{Z}_p[x]$ for $p = 3, 7, 11, 19, 23$ and is reducible for $p = 5, 13, 17$.

Looking for a general pattern, first note that each of the primes 5, 13 and 17 is of the form $4k + 1$, and on the contrary, none of the primes 3, 7, 11, 19 and 23 is in that form. Secondly, observe that

$$5 = 2^2 + 1^2,\ 13 = 3^2 + 2^2,\ 17 = 4^2 + 1^2,$$

while the primes 3, 7, 11, 19 and 23 don't enjoy such property, namely they cannot be represented as a sum of two squares. In fact one has the following beautiful theorem of Fermat:

An odd prime number p is a sum of two square, i.e., $p = a^2 + b^2$, if and only if it is of form $4k + 1$.

Also look at the solution of the problem 5.

Solution of the problem 2. Here is one example: $f(x) = 2x^2 + 4$. Note that $f(1) = f(2) = f(4) = f(5) = 0$. This does not contradict the theorem proven in class stating that a polynomial in $F[x]$ of degree d has at most d roots and the reason is simple: $\mathbb{Z}_6$ is not a field!

Solution of the problem 3. This can be done by a trial and error search and here is the answer:

$$[x^2 + x + 1]^{-1} = [x^2].$$

To verify our answer, notice that since $[x^3 + x + 1] = [0]$, we have

$$[x^2 + x + 1][x^2] = [x^4 + x^3 + x^2] = [x(-x - 1) + (-x - 1) + x^2] = [1]$$

(**N.B.** $2 = 0$ and $-1 = 1$, because we are working in $\mathbb{Z}_2$.) For another way of looking at this problem, go to the solution of the next problem.

Solution of the problem 4. Here you are:

$$[x]^1 = [x],\ [x]^2 = [x^2],\ [x]^3 = [x + 1],\ [x]^4 = [x^2 + x],$$

$$[x]^5 = [x^2 + x + 1],\ [x]^6 = [x^2 + 1],\ [x]^7 = [1].$$

So, the smallest $j > 0$ for which $[x]^j = [1]$ is 7, and therefore $[x]$ is a generator for the multiplicative group of nonzero elements of the finite field $\mathbb{Z}_2[x]/(x^3+x+1)$.

Back to the solution of the previous problem, note that

$$[x^2 + x + 1][x^2] = [x]^5[x]^2 = [x]^7 = [1]\ !$$

Solution of the problem 5. Proof by contradiction. Suppose that x^2+1 factors in $\mathbb{Z}_p[x]$. So, it has a root, a say, in $\mathbb{Z}_p$, i.e., $a^2+1=0$ in $\mathbb{Z}_p$. This in turn implies that $p \mid a^2+1$ or equivalently $a^2 \equiv -1 \pmod{p}$. Now since p is odd, we can raise both sides of $a^2 \equiv -1 \pmod{p}$ to the power $\dfrac{p-1}{2}$ to get

$$a^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Comparing with little Fermat, we infer that

$$1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Since $p>2$, this is impossible unless the last congruence relation becomes equality and that amounts to $\frac{p-1}{2}=2k$, hence $p=4k+1$, which is a contradiction!

Solution of the problem 6a. Let $R=F[X]$ where F is a field and let $I=F$ be the set of constant polynomials. Then I isn't an ideal because $i \in I \Leftrightarrow \deg(i)=0$ or $i=0$. So for any $f \in R$ s.t. $\deg(f) \geq 1$ and $0 \neq i \in I$ we have $\deg(f*i)=\deg(i)+deg(f) \geq 1 \Rightarrow f*i \notin I$.

Solution of the problem 6b. Let $R=\mathbb{Z}\times\mathbb{Z}$ and let $I=\{(m,0)|m \in \mathbb{Z}\}$. Then I is an ideal. Let $(a,0),(b,0) \in I$. Then $(a,0)+(b,0)=(a+b,0) \in I$, so I is closed under addition and if $(m,n) \in R$ is some arbitrary element we have that $(m,n)*(a,0)=(ma,0) \in I$ so I is closed under multiplication by arbitrary elements in R. It follows that I is an ideal.

Solution of the problem 6c. Let I be the set of nilpotent elements of a (commutative) ring R i.e.

$$I=\{a \in R|\exists\ m \in \mathbb{N} \text{ s.t. } a^m=0\}.$$

Then I is an ideal. Let $a,b \in I$, then $\exists m,n \in \mathbb{N}$ s.t. $a^m=b^n=0$. If $r \in R$ is some arbitrary element then $(ra)^m=r^m a^m=r^m 0=0$ (the second equality holds because R is commutative), so ra is also nilpotent, hence I is closed under multiplication by arbitrary elements. Now let $N=\max(n,m)$ and consider $(a+b)^{2N}$. First note that if $i \leq N$ then $2N-i \geq N$. So by the binomial theorem we have:

$$\begin{aligned}
(a+b)^{2N} &= \sum_{i=0}^{2N}\binom{2N}{i}a^i b^{2N-i} \\
&= \sum_{i=0}^{N}\binom{2N}{i}a^i \underbrace{b^{2N-i}}_{=0}+\sum_{i=N+1}^{2N}\binom{2N}{i}\underbrace{a^i}_{=0} b^{2N-i} \\
&= 0
\end{aligned}$$

It follows that $a+b$ is also nilpotent, so I is closed under addition, it follows that I is an ideal.

Remark It is important to notice that the statement of this problem is false if we remove the commutativity of R. Here is one example. Let $R = M_2[\mathbb{Z}]$ be the ring of all 2×2 integer matrices (with the usual addition and multiplication), and let

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

One easily sees that

$$A^2 = B^2 = O_2 \text{ (the zero matrix of size 2,)}$$

however, no positive power of $A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is zero! (check this). The reason behind this is that $M_2[\mathbb{Z}]$ is not a commutative ring.

For the next two parts, let R be the ring of functions from $\mathbb{Z}$ to $\mathbb{R}$ with addition $+_R$ and multiplication $*_R$. For $f, g \in R$, the addition $f +_R g \in R$ is defined as the mapping:

$$(f +_R g)(x) = f(x) + g(x)$$

and the product of two functions f and g is defined as the mapping:

$$(f *_R g)(x) = f(x)g(x).$$

From now on, subscripts for the operation signs will be omitted.

Solution of the problem 6d. Let I be the set of functions f s.t. $f(0) = f(1)$. I is not an ideal. Indeed, let $f \in I$ be the constant 1 function i.e. for each $n \in \mathbb{Z}, f(n) = 1$ and let g be the function $g(n) = n$. Then we have that $(f * g)(0) = f(0)g(0) = 1 \times 0 = 0$ but $(f * g)(1) = f(1)g(1) = 1$. So $f * g \notin I$ so I is not closed under multiplication by arbitrary elements of R so it's not an ideal.

Solution of the problem 6e. Let $I = \{f \in R | f(0) = f(1) = 0\}$. Let $f, g \in I$ then $(f+g)(1) = f(1)+g(1) = 0+0 = 0$ and similarly $(f+g)(0) = 0$ so I is closed under addition. Now let $h \in R$ be some arbitrary element. Then we find that $(h*f)(1) = h(1)f(1) = h(1)\times 0 = 0$ and $(h*f)(0) = h(0)f(0) = h(0)\times 0 = 0$, so $h * f \in I$. It follows that I is closed under multiplication by arbitrary elements of R. It follows that I is an ideal.

Solution of the problem 7. Let R be the polynomial ring $F[X]$ with coefficients in a field. Then all of its ideals are principal.

Remark. In class the strategy was to show that an ideal in $\mathbb{Z}$ is generated by its smallest positive element. Recall that in polynomial rings over fields, the notion of size corresponds to the degree of a polynomial.

Proof: Let $I \subset F[X] = R$ be an ideal. Then the set $S = \{n \in \mathbb{N} \ : \ n = \deg(f), \text{ fo some } f \in I\} \subset \mathbb{N}$ is nonempty (why?), so it must have a smallest element. If $0 \in S$ then I contains a constant $\Rightarrow I = R$. Otherwise let $s > 0$ be the smallest element in S. Then there is some $f \in I$ s.t. $\deg(f) = s$, i.e. f is the element of minimal degree in I.

Now we claim that $I = (f)$. On one hand $f \in I \Rightarrow (f) \subseteq I$. On the other hand, suppose $I \nsubseteq (f)$, then there is some $g \in I$ such that $f \nmid g$. So we can apply the division algorithm to get

$$g = fq + r$$

where $r \neq 0$ and $\deg(r) < \deg(f) = s$. But then we get $r = g - fq \in I$ because of closure of ideals under addition and multiplication. And we get that $m = \deg(r) \in S$ and $m < s$ contradiction minimality of s. It follows that $I = (f)$.