Math 31: Final Exam Practice

Date: 11/18/19

Test your knowledge

True/false questions

1. If A is a ring with n elements and $B \leq A$ a subring. Then $|B|$ divides n. ◯ True ◯ False
   True. If B is a subring, then it also forms a subgroup. Then apply Lagrange's Theorem.

2. If $\langle A, +, \cdot \rangle$ is a commutative ring. Then the cyclic subgroup $\langle x \rangle$ of $(A, +)$ is equal to the principal ideal $\langle x \rangle$ generated by x. ◯ True ◯ False
   False. Consider the commutative ring $\langle \mathbb{Q}, +, \cdot \rangle$ and let $x = 1/2$. Then the cyclic subgroup generated by x is
   $$\left\{k \cdot \frac{1}{2} : k \in \mathbb{Z}\right\}.$$
   The principal ideal generated by x is
   $$\left\{q \cdot \frac{1}{2} : q \in \mathbb{Q}\right\}.$$
   In particular, $1/4$ is in the principal ideal, but it is not in the cyclic subgroup.

3. There are finitely many irreducible polynomials in $\mathbb{Z}_5[x]$. ◯ True ◯ False
   False. We showed that $x^2 + 2$ is irreducible in $\mathbb{Z}_5[x]$. By Fermat's Little Theorem, it follows that $x^{2+5k} + 2$ is irreducible for $k \in \mathbb{N}$.

4. If $(A, +, \cdot)$ is an integral domain with $char(A) = p$, where p prime. Then A has p elements. ◯ True ◯ False
   False. $\mathbb{Z}_3[x]$ has infinitely many elements, but characteristic 3.

5. The principal ideal $\langle x^2 - 1 \rangle$ in $\mathbb{Z}[x]$ is a prime ideal. ◯ True ◯ False
   False. $(x + 1)(x - 1) = x^2 - 1 \in \langle x^2 - 1 \rangle$, but $x + 1 \notin \langle x^2 - 1 \rangle$.

6. Let A be a ring and J be an ideal of A. Every element of A/J is its own negative if and only if $x + x \in J$ for every $x \in A$. ◯ True ◯ False
   True. We have that:
   $$-(J + a) = J + a$$
   if and only if
   $$(J + a) + (J + a) = J + 0$$
   if and only if
   $$J + (a + a) = J + 0$$
   if and only if
   $$(a + a) \in J + 0 = J.$$

7. Every prime ideal of a commutative ring with unity is also a maximal ideal. ◯ True ◯ False
False. Consider the ideal $\{0\}$ of $\mathbb{Z}$ consisting only of the zero element. This is a prime ideal (since $\mathbb{Z}$ is an integral domain), but is not maximal (since it is contained in, for instance, the principal ideal generated by 5).

8. All the nonzero elements in a ring have the same additive order. ◯ True ◯ False
False. This is true for integral domains. However, in $\mathbb{Z}_6$, 2 and 3 have different additive orders.

9. In $\mathbb{Z}_3[x]$, $x+2$ is a factor of x^m+2 for all m. ◯ True ◯ False
True. It suffices to show that -2 is a root of x^m+2 for all m. Note that in $\mathbb{Z}_3$, $-2=1$. So we need to show that $1^m+2=0$ for all m. But this just means that $1+2=0$ in $\mathbb{Z}_3$, which is true.

10. Let A be an integral domain. If $(x+1)^2=x^2+1$ in $A[x]$, then A must have characteristic 2. ◯ True ◯ False
True. If $(x+1)^2=x^2+1$ in $A[x]$, then we have that $x^2+(1+1)x+1=x^2+1$. Using the Cancellation Property, we see that $(1+1)x=0$ in $A[x]$. Since $A[x]$ is an integral domain (because A is an integral domain), we have that either $1+1=0$ or $x=0$. However, $0\in A$ and $x\notin A$, so $x\neq 0$. Thus it must be that $1+1=0$ and A has characteristic 2.

Long answer questions

Question 1 Let $A \subseteq B$ where A and B are integral domains. Prove that A has characteristic p if and only if B has characteristic p.
Since A is a subring of B, it follows that the unity of B is the unity of A. Since subrings are closed under addition, the result is quickly implied.

Question 2 Compute the field of quotients for the integral domain $\mathbb{Z}_5[x]$.
Let

$$S = \{(a(x), b(x)) \mid a(x), b(x) \in \mathbb{Z}_5[x] \text{ and } b(x) \neq 0\}.$$

Define $(a(x), b(x)) \sim (c(x), d(x))$ to mean that $a(x)d(x) = b(x)c(x)$ as in the definition of the field of quotients. Then the equivalence classes are

$$[a(x), b(x)] = \{(c(x), d(x)) \mid a(x)d(x) = b(x)c(x)\}.$$

So the field of quotients is

$$A* = \{[a(x), b(x)] \mid a(x), b(x) \in \mathbb{Z}_5[x] \text{ and } b(x) \neq 0\}.$$

More concretely, this can be seen to be isomorphic to the ring of rational functions with coefficients in $\mathbb{Z}_5$.

Question 3 Let A be a commutative ring and suppose that a is an idempotent element of A (meaning that $a^2 = a$).

a) Show that the function $f_a : A \to A$ defined by $f_a(x) = ax$ is a ring homomorphism. Let $x, y \in A$. Then

$$f_a(x + y) = a(x + y) = ax + ay = f_a(x) + f_a(y),$$

where the middle equality is due to the distributive law in the ring A. We also have that

$$\begin{aligned} f_a(xy) &= a(xy) \\ &= a^2(xy) && \text{since } a \text{ is an idempotent element} \\ &= (ax)(ay) && \text{since } A \text{ is commutative and multiplication is associative} \\ &= f_a(x)f_a(y), \end{aligned}$$

as desired. So f_a is a homomorphism.

b) Describe the kernel and the range of f_a. Be as precise as possible.
We have that

$$\ker(f_a) = \{x \in A \mid f_a(x) = 0\} = \{x \in A \mid ax = 0\}.$$

(This is often called an "annihilator" since it is the set of all values which are "annihilated" by a.)
We also have that

$$\text{im}(f_a) = \{y \in A \mid f_a(x) = y \text{ for some } x \in A\} = \{y \in A \mid ax = y\}.$$

c) What does the Fundamental Homomorphism Theorem for rings say about these objects?
If we are careful, we can see that the function $g_a : A \to \text{im}(f_a)$ defined by $g_a(x) = f_a(x)$ is a surjective ring homomorphism with kernel equal to $\ker(f_a)$. So, by the FHT, we know that

$$A/\ker(f_a) \cong \text{im}(f_a)$$

.

Question 4 Show that if $p(x)$ is an irreducible polynomial in $F[x]$ (F is a field), then the principal ideal generated by $p(x)$ is a maximal ideal of $F[x]$.

Proof. The ideal $\langle p(x)\rangle$ is maximal if and only if $F[x]/\langle p(x)\rangle$ is a field. Since $F[x]$ is an integral domain, we already know that $F[x]/\langle p(x)\rangle$ is a commutative ring with unity. So it suffices to show that every nonzero element in $F[x]/\langle p(x)\rangle$ is invertible.

Let $\langle p(x)\rangle + a(x) \in F[x]/\langle p(x)\rangle$ with $\langle p(x)\rangle + a(x) \neq \langle p(x)\rangle + 0 = \langle p(x)\rangle$. Then $a(x) \notin \langle p(x)\rangle$. More specifically, this means that $a(x)$ is not a multiple of $p(x)$. Since $p(x)$ is irreducible, the only polynomials which divide $p(x)$ are constant polynomials (i.e., $d(x) = c \in F$) or $p(x)$ itself. Since $p(x)$ does not divide $a(x)$, the only common divisors of $p(x)$ and $a(x)$ are constant polynomials. Note that 1 is the unique monic polynomial associated to every constant polynomial, we conclude that $\gcd[p(x), a(x)] = 1$. Since the gcd is a linear combination of $a(x)$ and $p(x)$, there exist $b(x)$ and $q(x)$ such that

$$b(x)a(x) + q(x)p(x) = 1.$$

Rearranging, we see that

$$a(x)b(x) = (-q(x))p(x) + 1 \in \langle p(x)\rangle + 1.$$

Thus

$$(\langle p(x)\rangle + a(x))(\langle p(x)\rangle + b(x)) = \langle p(x)\rangle + (a(x)b(x)) = \langle p(x)\rangle + 1.$$

Therefor $\langle p(x)\rangle + a(x)$ is invertible. Since $\langle p(x)\rangle + a(x)$ was an arbitrary nonzero element in $F[x]/\langle p(x)\rangle$, we have that $F[x]/\langle p(x)\rangle$ is a field. Thus $\langle p(x)\rangle$ is maximal. □

Question 5 Determine if each of the following is irreducible.

1. $x^2 + x + 1$ in $\mathbb{Z}_2[x]$.
   There are only three monic reducible quadratic polynomials mod 2, because there are only 2 coefficients (0 and 1) to work with. You can easily list them all to check:

   $$(x + 1)(x + 1) = x^2 + 0x + 1 = x^2 + 1$$

   and

   $$(x + 1)x = x^2 + x$$

   and

   $$x \cdot x = x^2.$$

   Since the given polynomial is none of these, it must be irreducible.

2. $x^3 + x + 1$ in $\mathbb{Z}_3[x]$.
   Note that $1^3 + 1 + 1 = 0$ in $\mathbb{Z}_3$. (If you don't notice it right away, use Fermat's Little Theorem to solve.) Since the polynomial has 1 as a root, it has $(x - 1)$ (equivalently $(x + 2)$) as a factor. This implies that it's reducible. However, if you'd like to factor it, you can use polynomial

long division.

$$
\begin{array}{rrrrrr}
 & x^2 & +x & +2 & & \\
\hline
x \quad +2 \;) & x^3 & +0x^2 & +x & +1 & \\
 & -(x^3 & +2x^2) & & & \\
\hline
 & & 1x^2 & +x & & \\
 & & -(1x^2 & +2x) & & \\
\hline
 & & & 2x & +1 & \\
 & & & -(2x & +1) & \\
\hline
 & & & & 0 &
\end{array}
$$

So,

$$x^3 + x + 1 = (x + 2)(x^2 + x + 2).$$

3. $x^4 + 1$ in $\mathbb{Z}_{11}[x]$.
   If this is reducible, there are two possible options: either it has a root, or it is a product to two irreducible quadratics. Pursuing each option, and working out the resulting system of equations, we can find that can be factored as

$$(x^2 + 8x + 10)(x^2 + 3x + 10) = x^4 + 1.$$

   So the polynomial is reducible over $\mathbb{Z}_{11}$.

4. $x^4 + 10x^2 + 5$ in $\mathbb{Z}[x]$.
   Let $p = 5$. Then $p \mid 5$, $p \mid 10$, $p^2 \nmid 5$, and $p \nmid 1$. So by EIC, this polynomial is irreducible over $\mathbb{Z}$.