Math 113 Homework # 10 solutions

26.3. As discussed in class, the ideals in $\mathbb{Z}_{12}$ are the images, under the canonical homomorphism $\mathbb{Z} \to \mathbb{Z}_{12}$, of the ideals in $\mathbb{Z}$ containing $12\mathbb{Z}$, which are the ideals (d) where $d|12$, i.e. the ideals (1), (2), (3), (4), (6), and (12). The corresponding ideals in $\mathbb{Z}_{12}$ are $\mathbb{Z}_{12}$, $\{0, 2, 4, 6, 8, 10\}$, $\{0, 3, 6, 9\}$, $\{0, 4, 8\}$, $\{0, 6\}$, and $\{0\}$. We saw earlier that if $d|n$ then as groups, $\mathbb{Z}_n/\langle d\rangle \simeq \mathbb{Z}_d$. This isomorphism preserves multiplication and so is also a ring isomorphism. Thus the quotient rings of $\mathbb{Z}_{12}$ by the above ideals are isomorphic, respectively, to $\{0\}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_6$, and $\mathbb{Z}_{12}$.

26.10. (a) True, see the fundamental homomorphism theorem and the surrounding discussion.

(b) False. The inclusion map $\mathbb{Z} \to \mathbb{Q}$ does not send ideals to ideals, because $\mathbb{Z}$ is an ideal in $\mathbb{Z}$ but $\mathbb{Z}$ is not an ideal in $\mathbb{Q}$. ($\mathbb{Q}$ contains no nontrivial ideals since it is a field.)

(c) True, because a ring homomorphism is in particular a homomorphism of additive groups, and we know that this is true for homomorphisms of groups.

(d) False. $\mathbb{R}$ contains no ideals other than $\{0\}$ and $\mathbb{R}$ since $\mathbb{R}$ is a field. More explicitly, $\mathbb{Q}$ is not an ideal in $\mathbb{R}$ because $1 \in \mathbb{Q}$ and $\sqrt{2} \in \mathbb{R}$ but $\sqrt{2} \cdot 1 \notin \mathbb{Q}$.

(e) True by definition, as mentioned in class, since $RI \subset I$ implies $II \subset I$.

(f) False, e.g. $\mathbb{Z} \subset \mathbb{Q}$ or $\mathbb{Q} \subset \mathbb{R}$ as above.

(g) True, since if I is an ideal in a commutative ring then $(a+I)(b+I) = ab + aI + Ib + bI = ba + Ia + bI + Ib = (b + I)(a + I)$.

(h) True; this is how we defined $\mathbb{Z}_4$.

(i) True. ($\Rightarrow$) is immediate. To prove ($\Leftarrow$), note that if N is an ideal and $1 \in N$, then for any $x \in R$ we have $x = x \cdot 1$ so $x \in N$.

(j) True, a normal subgroup is a subgroup out of which you can make a quotient group, and an ideal is a subring out of which you can make a quotient ring.

26.15. The diagonal $\Delta = \{(x, x) \mid x \in Z\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$. (It's isomorphic to $\mathbb{Z}$.) However it is not an ideal because $(1, 1) \in \Delta$ and $(2, 3) \in \mathbb{Z} \times \mathbb{Z}$ but $(2, 3)(1, 1) = (2, 3) \notin \Delta$.

26.16c. If R/N is commutative, then for all $r, s \in R$ we have $[r][s] = [s][r]$ in R/N, so by definition of addition and multiplication in the quotient ring, $[rs - sr] = [0]$, so $rs - sr \in N$. Conversely, since every element of R/N is the equivalence class of some element of R, if $rs - sr \in N$ for all $r, s \in R$, then the above calculation shows that R/N is commutative.

26.22. (a) Let $x' \in \phi(N)$ and $y' \in \phi(R)$; we must show that $x'y' \in \phi(N)$. We can write $x' = \phi(x)$ with $x \in N$ and $y' = \phi(y)$ with $y \in R$. Since N is an ideal in R, we have $xy \in N$. Then since ϕ is a homomorphism, $x'y' = \phi(x)\phi(y) = \phi(xy)$ so $x'y' \in \phi(N)$.

(b) Let $R = \mathbb{Z}$ and $R' = \mathbb{Q}$, let ϕ be the inclusion map, and let $N = \mathbb{Z}$.

(c) Suppose N' is an ideal in $\phi(R)$; show $\phi^{-1}(N')$ is an ideal in R. Let $x \in \phi^{-1}(N')$ and $y \in R$; show $xy \in \phi^{-1}(N')$, i.e. $\phi(xy) \in N'$. Well, $\phi(xy) = \phi(x)\phi(y)$; since $\phi(x) \in N'$ and $\phi(x) \in \phi(R)$ and N' is an ideal in $\phi(R)$, it follows that $\phi(xy) \in N'$.

When N' is an ideal in R' instead of in $\phi(R)$, the proof is almost the same.

26.30. First we have to show that the nilpotent elements form an additive subgroup. Clearly 0 is nilpotent, and if a is nilpotent then $-a$ is nilpotent since if $a^n = 0$ then $(-a)^n = (-1)^n a^n = (-1)^n 0 = 0$. The tricky part is to show that if a and b are nilpotent then so is $a + b$. If $a^m = 0$ and $b^n = 0$, then we have the binomial expansion

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i}.$$

In each term of the right hand side, the exponent of a is at least m or the exponent of b is at least n (or both), since the total exponent is $m + n$. Thus all terms on the right hand side are zero, so $(a + b)^{m+n} = 0$, and $a + b$ is nilpotent. So the nilpotent elements form an additive subgroup, and to complete the proof that they comprise an ideal, we only need to check that if a is nilpotent and $x \in R$ then ax is nilpotent. To prove this we note that if $a^n = 0$, then $(ax)^n = a^n x^n = 0x^n = 0$. Note that we have used commutativity of R a lot in the above proof.

26.31. In $\mathbb{Z}_n$, the equivalence class $[x]$ is nilpotent if and only if some power of x is a multiple of n, if and only if every prime that divides n also divides x. (Can you see why?) So the nilradical of $\mathbb{Z}_{12}$ is $\{0, 6\}$, while the nilradical of $\mathbb{Z}_{32}$ is $\{0, 2, 4, 6, \ldots, 28, 30\}$. On the other hand, the nilradical of $\mathbb{Z}$ is $\{0\}$, since no power of a nonzero integer is zero.

27.6. $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$ is a field if and only if $x^3 + x^2 + c$ is irreducible over $\mathbb{Z}_3$ if and only if $x^3 + x^2 + c$ has no root in $\mathbb{Z}_3$. If $c = 0$ then $x = 0$ is a root; if $c = 1$ then $x = 1$ is a root. However, when $c = 2$, we check all three possibilities to see that x^3+x^2+2 has no roots. So for $c \in \mathbb{Z}_3$, the ring $\mathbb{Z}_3[x]/(x^3+x^2+c)$ is a field if and only if $c=2$.

27.14. (a) False. The ideal $\{0\}$ in $\mathbb{Z}$ is prime but not maximal.

(b) True, as explained in class, because every field is an integral domain.

(c) True.

(d) False, it's $\mathbb{Q}$.

(e) True, by Theorem 27.19.

(f) True, e.g. $\mathbb{Q} \times \mathbb{Q}$ has zero divisors since $(1,0)\cdot(0,1)=0$, but the subring $\mathbb{Q} \times \{0\}$ is isomorphic to $\mathbb{Q}$.

(g) True, as explained in class and in Theorem 27.19.

(h) False. The fact that $F[x]$ has no zero divisors just shows that the ideal $\{0\}$ is prime in $F[x]$. However the ideal (x^2) is not prime, since $x \cdot x \in (x^2)$ but $x \notin (x^2)$.

(i) True, as proved in class and Theorem 27.24.

(j) False, e.g. (x^2) is principal but not maximal since the ideal (x) is between (x^2) and $F[x]$.

27.15. If p is prime then $Z \times p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z} \times \mathbb{Z}$.

27.16. The ideal $\mathbb{Z} \times \{0\}$ in $\mathbb{Z} \times \mathbb{Z}$ is prime but not maximal.

45.10. In $\mathbb{Z}[x]$, the factorization into irreducibles is $2^2(x^2-x+2)$. In $\mathbb{Q}[x]$ it is already irreducible. In $\mathbb{Z}_{11}[x]$ the factorization into irreducibles is $(x-5)(4x+5)$. (And in $\mathbb{Z}_{11}[x]$ there are 9 other factorizations into irreducibles, obtained by multiplying one factor by c and the other factor by c^{-1} where $c \in \mathbb{Z}_{11}^*$.)

27.38. Let I be an ideal of $M_2(\mathbb{Z}_2)$ and suppose that $I \neq \{0\}$, i.e. I contains a nonzero matrix A. We must show that $I = M_2(\mathbb{Z}_2)$. If A is invertible then this is immediate, because $1 \in I$. If A is not invertible, then without loss of generality, by changing coordinates, we may assume that $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. (I'll leave the details of this as an exercise in linear algebra review.) Then I contains $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and $A \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, so it contains their sum $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, which is invertible.

In the above argument we could replace $\mathbb{Z}_2$ with any field and it would still go through. With a bit more work one can show that $M_n(F)$ is simple.