Math 60210, Basic Algebra, Problem Set 8, Fall 2018
due Wed, October 31

Do 8 of these 12 problems. Everyone should read 5, 9, and 10 and remember the notation. As in class, $R[x]$ is the polynomial ring with coefficients in R.

1. (A) Let R be a ring. An element $x \in R$ is called nilpotent if $x^n = 0$ for some $n > 0$. If $x \in R$ is nilpotent, prove that $1 + x \in R^*$.

(B) If F is a field and $A \in M(n, F)$ has the property that the entries $A_{i,j} = 0$ for $i \geq j$, prove that $(I + A)$ is invertible and give a formula for $(I + A)^{-1}$.

2. Let d be a square-free integer, i.e., $d \neq 1$ and m^2 does not divide d for every integer $m \geq 2$. Let $E = \mathbf{Q}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbf{Q}\}$. Prove that E is a subring of $\mathbf{C}$. Is E a field? Explain why or why not.

3. Let d be a square-free integer not equal to 1. Let $R = \mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbf{Z}\}$.

(i) Prove that R is a subring of $\mathbf{C}$.

(ii) Let $N(\alpha) = \alpha \cdot \tau(\alpha)$, where for $\alpha = a + b\sqrt{d} \in R$, $\tau(\alpha) = a - b\sqrt{d}$. Prove that $N(\alpha) \in \mathbf{Z}$, and $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$ for all $\alpha, \beta \in R$.

(iii) Let $d < 0$. Compute the unit group R^* of R if $d < 0$ (hint: show $\alpha \in R^*$ if and only if $N(\alpha) = 1$).

4. Let $\zeta = e^{2\pi i/3}$. Let $R = \{a + b\zeta : a, b \in \mathbf{Z}\}$. Prove that R is a subring of $\mathbf{C}$ and compute the unit group R^*. Does R contain any of the rings $\mathbf{Z}[\sqrt{d}]$ from Problem 4. If so, which one?

5. Let R be a ring, and let $R^\times$ be the set of all units of R. Prove that $R^\times$ is a group under multiplication.

6. (i) Let R be an integral domain. Prove that the unit group $R[x]^\times$ of $R[x]$ is $R^\times$.

(ii) Let R be a ring with nonzero (nilpotent) element a with $a^n = 0$ for some n. Prove that $1 - ax$ is a unit of $R[x]$.

7. Let F be a field. Prove that if $f = \sum_{i=0}^{\infty} a_i x^i \in F[[x]]$, then f is a unit if and only if $a_0 \neq 0$. Can you find the unit group of $R[[x]]^\times$ for an integral domain R?

8. Let $\mathbf{H}$ be the quaternions, i.e.,

$$\mathbf{H} = \{A \in M(2, \mathbf{C}) : A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}\},$$

and for A as above, we call α and β the coordinates of A. We said in class that $\mathbf{H}$ is a subring of the two by two complex matrices $M(2, \mathbf{C})$, and $\mathbf{H}$ is a real subspace of $M(2, \mathbf{C})$ with basis $\mathbf{1}, \mathbf{I}, \mathbf{J}, \mathbf{K}$, where $\mathbf{1}$ is the 2 by 2 identity matrix,

$$\mathbf{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ \mathbf{J} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \mathbf{K} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

We defined $N(A) = \frac{1}{2}\mathrm{Tr}(A \cdot -\overline{A}^{tr}) = |\alpha|^2 + |\beta|^2$ for A with coordinates α, β.

(i) For $A, B \in \mathbf{H}$, prove that $N(A \cdot B) = N(A) \cdot N(B)$.

(ii) Let $\mathbf{H}_1 := \{A \in \mathbf{H} : N(A) = 1\}$. Prove that H_1 is a group using the multiplication in $\mathbf{H}$ (the group $\mathbf{H}_1$ is often called $SU(2)$, the determinant one unitary 2 by 2 matrices).

(iii) Prove that center $Z(\mathbf{H}) = \mathbf{R} \cdot \mathbf{1}$, i.e., the real multiples of the identity matrix.

9. Let R be a ring and let $a \in R$. Let $C_R(a) = \{x \in R : xa = ax\}$. Prove that $C_R(a)$ is a subring of R.

10. Let R be a ring and let $\{S_i\}_{i\in I}$ be a family of subrings of R. Prove that $\cap_{i\in I} S_i$ is a subring of R. Let $Z(R) = \{x \in R : xy = yx, \ \forall \ y \in R\}$ ($Z(R)$ is called the center of R). Show $Z(R) = \cap_{a\in R} C_R(a)$, so $Z(R)$ is a subring of R.

11. Let F be the free group on a set S with two elements and let x and y be the generators of F corresponding to elements of S. Fix $n > 0$, and let $A(n) = F/N$, where N is the smallest normal subgroup of F containing x^n, y^2, and $yxy^{-1}x$.

(i) Let $a = xN$ and let $b = yN$. Prove that every element of $A(n)$ can be written in the form $a^i b^j$, where $i = 0, \ldots, n-1$ and $j = 0, 1$, and conclude that $|A(n)| \leq 2n$.

(ii) Prove that $A(n) \cong D_{2n}$ (hint: there is a surjective homomorphism from F to D_{2n}).

12. Let $R = M(n, F)$, where F is a field. Let I be a two-sided ideal of R. Prove that either $I = 0$ or $I = R$ (hint: $aI \subset I$ and $Ia \subset I$ for every $a \in R$. Use elementary matrices).