Math 241, Introduction to Abstract Algebra – Fall 2019
Course website: `https://sites.aub.edu.lb/kmakdisi/`
Problem set 11, NOT DUE — use for review

Reminder: Check out the Fall 2011 final for Math 241 for additional exercises on ring theory (and, of course, also on groups). The final is available from the Jafet library website, section "Course Reserves". You can search for Math 241 from the page

`http://library.aub.edu.lb/search/r`

Exercises from Fraleigh:

Section 27, exercises 6, 18, 19, 32.
Section 22, exercises 3, 4, 5, 9, 11, 12, 14, 15, 27 (also prove $D(fg) = fD(g) + gD(f)$).
Section 23, exercises 2, 4, 7, 10, 12, 13, 27, 28, 29, 34, 35.

Additional Exercises:

Exercise A11.1: a) Find the factorization of $x^p - x$ in $\mathbf{Z}_p[x]$, where p is a prime.
b) What are the roots of $x^3 - x$ in $\mathbf{Z}_6$?

Exercise A11.2: Let R be a ring which contains a field $F \subset R$ as a subring. (Example: $R = F[x]$.) Let I be a proper ideal of R. Show that R/I also contains a subring isomorphic to F.

Exercise A11.3: Show that in $F[x]$ the quotient and remainder for polynomial division are unique. So $f = qg + r$ with q, r unique once $\deg r < \deg g$. (Hint: degree of $r - r'$ if $f = qg + r = q'g + r'$.) Deduce that the quotient ring $R/\langle g\rangle$ not only contains a subring isomorphic to F as in the above exercise, but that $R/\langle g\rangle$ is a vector space over F of the same dimension as $\deg g$.

Exercise A11.4: Continuing the ideas above: show that:
a) $\mathbf{R}[x]/\langle x^2 + 1\rangle$ is a field, isomorphic to $\mathbf{C}$,
b) $\mathbf{R}[x]/\langle x^2 + x + 1\rangle$ is also a field isomorphic to $\mathbf{C}$,
c) $\mathbf{R}[x]/\langle x^2 - 2\rangle$ is not a field, and in fact is isomorphic to the product ring $\mathbf{R} \times \mathbf{R}$ (there are zero divisors; can you describe them explicitly as cosets $f + \langle x^2 - 2\rangle$?
d) $\mathbf{Q}[x]/\langle x^2 - 2\rangle$ is a field, isomorphic to $\{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ which is a subfield of $\mathbf{R}$,
e) $\mathbf{Z}_3[x]/\langle x^2 + 1\rangle$ is a field with 9 elements,
f) $\mathbf{Z}_2[x]/\langle x^2 + 1\rangle$ is not a field,
g) $\mathbf{Z}_2[x]/\langle x^3 + x + 1\rangle$ is a field with 8 elements.

Further "Look at" exercises:

Section 27, exercises 15–17, 25–27, 36–38.
Section 23, exercises 14–17, 22 (also: if the polynomial were $6x^4 + 17x^3 + 7x^2 + x - 9$, how many real roots would it have?), 31, 37.

"Look At" Exercise L11.1: a) Show that A_5 is a simple group by showing that if $N \triangleleft A_5$ with $N \neq \{1\}$, then N is a union of conjugacy classes of A_5 (whose cardinalities you know from a previous exercise), and that no such union can have cardinality that is a divisor of $60 = |A_5|$ unless the union consists of all of A_5.

b) Show that, for $n \geq 6$, the group A_n is simple by reducing to the case A_{n-1}. Idea: let N be as above and take $\sigma \in N, \sigma \neq 1$. If $\sigma(i) = i$ for some i, then σ belongs to a subgroup isomorphic to A_{n-1}, and so conjugates of σ generate that entire subgroup, and conjugates of such elements generate all of A_n. On the other hand, if σ moves all elements around, find $\tau \in A_n$ which satisfies $\tau\sigma\tau^{-1}(1) = \sigma(1)$ but $\tau\sigma\tau^{-1} \neq \sigma$, from which $\sigma^{-1}\tau\sigma\tau^{-1}$ is a nontrivial element of N which fixes 1, and you are back in the previous case.

"Look At" Exercise L11.2: Generalize the proof technique of Exercise A9.2 to show the existence of p-Sylow subgroups by induction on $|G|$. Hint: if $|Z|$ is divisible by p, let $a \in Z$ have order p, and show that $\langle a\rangle \triangleleft G$. Then do something using a Sylow subgroup of $G/\langle a\rangle$. Otherwise, some nontrivial conjugacy class C_x has cardinality prime to p, and a Sylow subgroup of Z_x does the trick.

"Look At" Exercise L11.3: Try to find Sylow p-subgroups of S_p (easy), S_{p^2} (hint: there is a subgroup isomorphic to $S_p \times \cdots \times S_p$, p times, and now take the group generated by a Sylow subgroup of each S_p factor and also by another element of order p that moves the different S_p factors around), S_{p^k} for $k \geq 3$ (hint: imitate the technique for S_{p^2}). You may want to look up "wreath products" of groups.